Administrar VMware vSAN

VMware vSphere 6.5
VMware vSAN 6.6.1

Puede encontrar la documentación técnica más actualizada en el sitio web de WMware en:

https://docs.vmware.com/es/

En el sitio web de VMware también están disponibles las últimas actualizaciones del producto.

Si tiene algún comentario sobre esta documentación, envíelo a la siguiente dirección de correo electrónico:

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

VMware, Inc.
Paseo de la Castellana 141. Planta 8.
28046 Madrid.
Tel.:+ 34 91 418 58 01
Fax: + 34 91 418 50 55
www.vmware.com/es

Contenido

Acerca de VMware vSAN

En *Administrar VMwarevSAN* se explica cómo configurar, administrar y supervisar un clúster de VMware vSAN en un entorno de VMware vSphere®. Además, en *Administrar VMwarevSAN* se explica cómo organizar los recursos locales de almacenamiento físico que funcionan como dispositivos de capacidad de almacenamiento en un clúster de vSAN, definir directivas de almacenamiento para máquinas virtuales implementadas en almacenes de datos de vSAN y administrar errores en un clúster de vSAN.

Audiencia prevista

Esta información está destinada a administradores de virtualización experimentados que están familiarizados con la tecnología de virtualización, las operaciones cotidianas de los centros de datos y los conceptos de vSAN.

vSphere Client HTML5 para vSAN

vSphere Client vSphere Client es un nuevo cliente basado en HTML5 que se incluye junto con vCenter Server en vSphere Web Client. El nuevo vSphere Client usa muchos términos, topologías y flujos de trabajo de la interfaz de vSphere Web Client. Sin embargo, el vSphere Client no admite vSAN. Los usuarios de vSAN deben seguir utilizando vSphere Web Client para esos procesos.

NOTA: No todas las funcionalidades de vSphere Web Client se implementaron para vSphere Client en la versión de vSphere 6.5. Para obtener una lista actualizada de las funcionalidades no compatibles, consulte la *Guía sobre actualizaciones de las funcionalidades en vSphere Client* en http://www.vmware.com/info?id=1413.

Introducción a vSAN

1

VMware vSAN es una capa distribuida de software que se ejecuta de manera nativa como parte del hipervisor de ESXi. vSAN agrega dispositivos de capacidad locales o con conexión directa de un clúster de host y crea un grupo de almacenamiento individual compartido entre todos los hosts del clúster de vSAN.

vSAN admite las características de VMware que requieren almacenamiento compartido (como HA, vMotion y DRS) y, al mismo tiempo, elimina la necesidad de usar almacenamiento compartido externo y simplifica las actividades de aprovisionamiento de máquinas virtuales y configuración de almacenamiento.

Este capítulo cubre los siguientes temas:

Conceptos de vSAN

VMware vSAN emplea un enfoque definido por software que crea almacenamiento compartido para máquinas virtuales. Virtualiza los recursos locales de almacenamiento físico de los hosts ESXi y los transforma en grupos de almacenamiento que pueden dividirse y asignarse a máquinas virtuales y aplicaciones en función de sus requisitos de calidad de servicio. vSAN se implementa directamente en el hipervisor de ESXi.

Puede configurar vSAN para que funcione como un clúster híbrido o basado íntegramente en tecnología flash. En clústeres híbridos, se utilizan dispositivos flash para la capa de almacenamiento en caché y discos magnéticos para la capa de capacidad de almacenamiento. En los clústeres basados íntegramente en tecnología flash, los dispositivos flash se utilizan para memoria caché y de capacidad.

Puede activar vSAN en sus clústeres de host existentes y cuando cree clústeres nuevos. vSAN agrega todos los dispositivos de capacidad a un solo almacén de datos compartido por todos los hosts del clúster de vSAN. Puede expandir el almacén de datos agregando dispositivos de capacidad o hosts con dispositivos de capacidad al clúster. vSAN funciona mejor cuando todos los hosts ESXi del clúster comparten configuraciones similares o idénticas entre todos los miembros del clúster, lo que incluye configuraciones similares o idénticas para el almacenamiento. Esta configuración coherente equilibra los componentes de almacenamiento de máquinas virtuales en todos los dispositivos y hosts del clúster. Los hosts sin dispositivos locales también pueden participar y ejecutar sus máquinas virtuales en el almacén de datos de vSAN.

Si un host aporta sus dispositivos de almacenamiento local a un almacén de datos de vSAN, debe proporcionar al menos un dispositivo para la memoria caché flash y al menos un dispositivo para capacidad. Los dispositivos de capacidad también se denominan discos de datos.

Los dispositivos del host que aporta los dispositivos forman un grupo de discos o más. Cada grupo de discos contiene un dispositivo flash de almacenamiento en caché y un dispositivo de capacidad, o varios, para almacenamiento persistente. Cada host puede configurarse para emplear varios grupos de discos.

Para obtener información sobre prácticas recomendadas, consideraciones de capacidad y recomendaciones generales sobre el diseño y el dimensionamiento de un clúster de vSAN, consulte la *guía de diseño y dimensionamiento de VMware vSAN*.

Características de vSAN

En este tema se resumen las características que se aplican a vSAN, sus clústeres y almacenes de datos.

vSAN ofrece varias ventajas a su entorno.

Tabla 1-1. Características de vSAN

Funciones compatibles	Descripción
Compatibilidad con almacenamiento compartido	vSAN es compatible con funciones de VMware que requieren almacenamiento compartido, como HA, vMotion y DRS. Por ejemplo, si un host está sobrecargado, DRS puede migrar máquinas virtuales a otros hosts del clúster.
Un montón de discos (JBOD)	vSAN admite JBOD para uso en un entorno de servidores blade. Si el clúster contiene servidores blade, puede extender la capacidad del almacén de datos mediante almacenamiento JBOD conectado a los servidores blade.
Formato en disco	vSAN 6.6 es compatible con el formato de archivo virtual en disco 5.0, que admite una administración de instantáneas y clones muy escalable por cada clúster de vSAN. Para obtener información sobre la cantidad de instantáneas y clones de máquinas virtuales que se admite por cada clúster de vSAN, consulte el documento *Valores máximos de configuración*.
Configuraciones híbridas y basadas íntegramente en tecnología flash	vSAN puede configurarse para un clúster híbrido o basado íntegramente en tecnología flash.
Dominios de errores	vSAN admite la configuración de dominios de errores para proteger a los hosts contra errores de los bastidores o los chasis cuando el clúster de vSAN abarca varios bastidores o chasis de servidores blade en un centro de datos.
Clúster ampliado	vSAN admite clústeres ampliados que abarcan dos ubicaciones geográficas.
vSAN Health Service	vSAN Health Service incluye pruebas de comprobación de estado configuradas previamente para supervisar, solucionar problemas, diagnosticar causas de problemas de componentes del clúster e identificar riesgos posibles.
Servicio de rendimiento de vSAN	En el servicio de rendimiento de vSAN, se incluyen tablas estadísticas utilizadas para supervisar las E/S por segundo, el rendimiento, la latencia y la congestión. Puede supervisar el rendimiento de un clúster de vSAN, un host, un grupo de discos, un disco y máquinas virtuales.
Integración con las funciones de almacenamiento de vSphere	vSAN se integra con las funciones de administración de datos de vSphere utilizadas tradicionalmente con el almacenamiento VMFS y NFS. Estas funciones incluyen instantáneas, clones vinculados, vSphere Replication y las API de vSphere para la protección de datos.

Tabla 1-1. Características de vSAN (Continua)

Funciones compatibles	Descripción
Directivas de almacenamiento de máquinas virtuales	vSAN funciona con las directivas de almacenamiento de máquina virtual para admitir un enfoque centrado en máquinas virtuales en la administración de almacenamiento. Si no se asigna una directiva de almacenamiento a la máquina virtual durante la implementación, se asigna automáticamente la directiva de almacenamiento predeterminada de vSAN a la máquina virtual.
Aprovisionamiento rápido	vSAN permite el aprovisionamiento rápido de almacenamiento en vCenter Server® durante las operaciones de creación e implementación de máquinas virtuales.

Términos y definiciones de vSAN

vSAN introduce términos y definiciones específicos que resulta importante comprender.

Antes de comenzar con vSAN, revise los términos y definiciones clave de vSAN.

Grupo de discos

Un grupo de discos es una unidad de capacidad de almacenamiento físico en un host y un grupo de dispositivos físicos que proporcionan rendimiento y capacidad al clúster de vSAN. En cada host ESXi que aporta sus dispositivos locales a un clúster de vSAN, los dispositivos se organizan en grupos de discos.

Cada grupo de discos debe tener un dispositivo flash de almacenamiento en caché y un dispositivo de capacidad, o varios. Los dispositivos utilizados para el almacenamiento en caché no pueden compartirse entre los grupos de discos ni tampoco pueden utilizarse para otras finalidades. Cada dispositivo de almacenamiento en caché debe estar dedicado a un solo grupos de discos. En clústeres híbridos, se utilizan dispositivos flash para la capa de almacenamiento en caché y discos magnéticos para la capa de capacidad de almacenamiento. En un clúster basado íntegramente en tecnología flash, los dispositivos flash se utilizan para la memoria caché y la capacidad. Para obtener información sobre la creación y la administración de grupos de discos, consulte Capítulo 10, “Administrar dispositivos en un clúster de vSAN,” página 109.

Capacidad utilizada

La capacidad utilizada es la cantidad de capacidad física utilizada por una máquina virtual o más en cualquier momento dado. Existen muchos factores que determinan la capacidad utilizada, incluidos el tamaño utilizado de los VMDK, las réplicas de protección, etc. Al calcular el tamaño de la memoria caché, no tenga en cuenta la capacidad utilizada para las réplicas de protección.

Almacenamiento basado en objetos

vSAN almacena y administra datos en contenedores flexibles de datos denominados objetos. Un objeto es un volumen cuyos datos y metadatos se distribuyen en el clúster. Por ejemplo, cada VMDK constituye un objeto, al igual que cada instantánea. Al aprovisionar una máquina virtual en un almacén de datos de vSAN, vSAN crea un conjunto de objetos compuesto por varios componentes para cada disco virtual. También crea el espacio de nombres del directorio principal de la máquina virtual, el cual es un objeto contenedor que almacena todos los archivos de metadatos de la máquina virtual. Según la directiva de almacenamiento de máquina virtual que se asignó, vSAN aprovisiona y administra cada objeto de manera individual, proceso que también puede incluir la creación de una configuración de RAID para cada objeto.

Cuando vSAN crea un objeto para un disco virtual y determina cómo distribuir el objeto en el clúster, considera los siguientes factores:

- vSAN comprueba que se apliquen los requisitos de discos virtuales de acuerdo con la configuración especificada para la directiva de almacenamiento de máquinas virtuales.

- vSAN comprueba que se utilicen los recursos de clúster correctos durante el aprovisionamiento. Por ejemplo, en función de la directiva de protección, vSAN determina cuántas réplicas se deben crear. La directiva de rendimiento determina la cantidad de Flash Read Cache para cada réplica y, asimismo, la cantidad de fracciones que se deben crear para cada réplica y dónde se deben ubicar dentro del clúster.
- vSAN supervisa e informa constantemente del estado de cumplimiento de la directiva para el disco virtual. Si encuentra cualquier estado que incumple la directiva, debe realizar un procedimiento de solución de problemas y resolver el problema subyacente.

NOTA: Cuando sea necesario, puede editar la configuración de la directiva de almacenamiento de la máquina virtual. La modificación de la configuración de la directiva de almacenamiento no afecta el acceso de la máquina virtual. vSAN regula de manera activa los recursos de red y almacenamiento que se utilizan para la reconfiguración, a fin de reducir el impacto de la reconfiguración de objetos en las cargas de trabajo normales. Cuando se modifica la configuración de la directiva de almacenamiento de máquina virtual, es posible que vSAN inicie un proceso de recreación de objetos y la resincronización posterior. Consulte "Acerca de la resincronización del clúster de vSAN," página 148.

- vSAN comprueba que los componentes de protección necesarios, como los reflejos y los testigos, se coloquen en dominios de errores o en hosts separados. Por ejemplo, para recompilar componentes durante un error, vSAN busca hosts ESXi que cumplan con las reglas de colocación en las que los componentes de protección de objetos de máquinas virtuales deben colocarse en dos hosts diferentes o en dominios de error.

Almacén de datos de vSAN

Después de habilitar vSAN en un clúster, se crea un solo almacén de datos de vSAN. Se muestra como otro tipo de almacén de datos en la lista de los almacenes de datos que pueden estar disponibles, incluidos los volúmenes virtuales, VMFS y NFS. Un solo almacén de datos de vSAN puede proporcionar distintos niveles de servicio para cada máquina o disco virtuales. En vCenter Server®, se muestran las características de almacenamiento del almacén de datos de vSAN como un conjunto de funcionalidades. Al definir una directiva de almacenamiento para máquinas virtuales, puede hacer referencia a estas funcionalidades. Cuando se implementan máquinas virtuales posteriormente, vSAN utiliza esta directiva para colocar las máquinas virtuales en el modo óptimo en función de los requisitos de cada máquina virtual. Para obtener información general sobre el uso de las directivas de almacenamiento, consulte el documento *Almacenamiento de vSphere* .

Un almacén de datos de vSAN posee características específicas que se deben considerar.

- vSAN proporciona un solo almacén de datos de vSAN, al que pueden acceder todos los hosts del clúster, independientemente de si aportan almacenamiento o no al clúster. Cada host puede montar cualquier otro tipo de almacenes de datos, incluidos los volúmenes virtuales, VMFS y NFS.
- Puede usar Storage vMotion para transferir máquinas virtuales entre los almacenes de datos de vSAN, de NFS y de VMFS.
- Solo los discos magnéticos y los dispositivos flash utilizados para capacidad pueden aportar capacidad al almacén de datos. Los dispositivos utilizados para la memoria caché flash no cuentan como parte del almacén de datos.

Objetos y componentes

Cada objeto consta de un conjunto de componentes, determinado por las funcionalidades utilizadas en la directiva de almacenamiento de máquina virtual. Por ejemplo, si **Nivel primario de errores que se toleran** se establece como 1, vSAN garantiza que los componentes de protección (como las réplicas y los testigos) se coloquen en hosts separados del clúster de vSAN, en el que cada réplica es un componente de un objeto. Además, en la misma directiva, si el valor configurado para el **número de fracciones de disco por objeto** es de dos o más, vSAN también fracciona el objeto en varios dispositivos de capacidad y cada fracción se considera un componente del objeto especificado. Cuando es necesario, vSAN también puede dividir los objetos grandes en varios componentes.

Un almacén de datos de vSAN contiene los siguientes tipos de objeto:

Espacio de nombres del directorio principal de la máquina virtual
El directorio principal de máquina virtual en el que se almacenan todos los archivos de configuración de máquina virtual, como `.vmx`, los archivos de registro, los VMDK y los archivos de descripción delta de instantáneas.

VMDK
Un disco de máquina virtual o un archivo `.vmdk` que almacena el contenido de la unidad de disco duro de las máquinas virtuales.

Objeto de intercambio de máquina virtual
Se crea cuando la máquina virtual está encendida.

VMDK delta de instantáneas
Se crean cuando se crean instantáneas de la máquina virtual.

Objeto de memoria
Se crea cuando está seleccionada la opción de memoria de instantánea al crear o suspender una máquina virtual.

Estado de cumplimiento de la máquina virtual: compatible y no compatible

Se considera que una máquina virtual está en estado de incumplimiento cuando uno de sus objetos o más no cumplen con los requisitos de la directiva de almacenamiento asignada. Por ejemplo, el estado puede pasar a ser de incumplimiento cuando no es posible acceder a una de las copias reflejadas. Si las máquinas virtuales cumplen con los requisitos definidos en la directiva de almacenamiento, el estado de las máquinas virtuales es de cumplimiento. Desde la pestaña **Physical Disk Placement** (Ubicación de discos físicos) de la página Virtual Disks (Discos virtuales), puede comprobar el estado de cumplimiento de la máquina virtual. Para obtener información sobre la solución de problemas de un clúster de vSAN, consulte "Controlar errores en vSAN," página 170.

Estado del componente: estados degradado y ausente

vSAN reconoce los siguientes estados de error para los componentes:

- Degraded (Degradado). Un componente entra en estado degradado cuando vSAN detecta un error permanente de un componente y determina que dicho componente no podrá recuperar su estado de funcionamiento original. En consecuencia, vSAN comienza a recompilar los componentes degradados de inmediato. Este estado puede producirse cuando un componente se encuentra en un dispositivo que genera un error.
- Absent (Ausente). Un componente entra en estado ausente cuando vSAN detecta un error temporal de un componente en el que el componente (incluidos todos sus datos) puede recuperarse y restaurar el estado original de vSAN. Este estado puede producirse cuando se reinician hosts o al desconectar un dispositivo de un host vSAN. vSAN espera 60 minutos antes de comenzar a recompilar los componentes en estado ausente.

Estado del objeto: correcto e incorrecto

Según el tipo y la cantidad de errores en el clúster, un objeto puede tener uno de los siguientes estados:

- Healthy (Estado correcto). Cuando hay disponible al menos un reflejo completo de RAID 1, o está disponible la cantidad mínima requerida de segmentos de datos, se considera que el objeto tiene un estado correcto.
- Unhealthy (Estado incorrecto). Se considera que un objeto tiene un estado incorrecto cuando no hay reflejos completos disponibles o el número mínimo requerido de segmentos de datos no está disponible para los objetos de RAID 5 o RAID 6. Si menos del 50 % de los votos de un objeto están disponibles, el objeto tiene un estado incorrecto. Varios errores en el clúster pueden provocar que los objetos entren en un estado incorrecto. Cuando un objeto tiene un estado operativo incorrecto, afecta la disponibilidad de la máquina virtual asociada.

Testigo

Un testigo es un componente que contiene únicamente metadatos y no datos reales de aplicaciones. Sirve como factor determinante cuando se debe tomar una decisión en relación con la disponibilidad de los componentes del almacén de datos restantes después de un error potencial. Un testigo utiliza aproximadamente 2 MB de espacio para metadatos en el almacén de datos de vSAN cuando se utiliza el formato en disco 1.0, y consume 4 MB para el formato en disco de la versión 2.0 y versiones posteriores.

vSAN 6.0 y versiones posteriores mantienen quórum mediante un sistema de votación asimétrico en el que cada componente puede tener más de un voto para decidir la disponibilidad de los objetos. Para que un objeto se considere disponible, la accesibilidad de los votos que componen el objeto de almacenamiento de una máquina virtual debe ser superior al 50 % en todo momento. Cuando la cantidad de votos a los que todos los hosts pueden acceder es igual o inferior al 50 %, el almacén de datos de vSAN ya no puede acceder al objeto. Los objetos inaccesibles pueden afectar la disponibilidad de la máquina virtual asociada.

Administrar el almacenamiento basada en directivas (SPBM)

Al usar vSAN, puede definir requisitos de almacenamiento de máquinas virtuales, como el rendimiento y la disponibilidad, mediante una directiva. vSAN garantiza que a las máquinas virtuales implementadas en los almacenes de datos de vSAN se les asigne, al menos, una directiva de almacenamiento de máquinas virtuales. Cuando se conocen los requisitos de almacenamiento de las máquinas virtuales, es posible crear directivas de almacenamiento y asignar las directivas a las máquinas virtuales. Si no se aplica una directiva de almacenamiento al implementar las máquinas virtuales, vSAN asigna de manera automática una directiva predeterminada de vSAN con el atributo **Nivel primario de errores que se toleran** configurado en uno, una sola fracción de disco para cada objeto y un disco virtual con aprovisionamiento fino. Para obtener mejores resultados, defina sus propias directivas de almacenamiento de máquinas virtuales, aunque los requisitos de sus directivas sean iguales a los que se definen en la directiva de almacenamiento predeterminada. Para obtener información sobre el uso de directivas de almacenamiento de vSAN, consulte Capítulo 12, “Usar las directivas de vSAN,” página 135.

Ruby vSphere Console (RVC)

Ruby vSphere Console (RVC) es una interfaz de línea de comandos que se utiliza para la administración y la solución de problemas del clúster de vSAN. RVC ofrece una vista integral del clúster, a diferencia de la vista centrada en hosts que proporciona `esxcli`. RVC está integrado en vCenter Server Appliance y vCenter Server para Windows, por lo tanto, no es necesario que lo instale por separado. Para obtener información sobre los comandos de RVC, consulte la *Guía de referencia de los comandos de RVC*.

vSphere PowerCLI

VMware vSphere PowerCLI incluye compatibilidad con scripts de línea de comandos para vSAN, que le ayudarán a automatizar las tareas de administración y configuración. vSphere PowerCLI proporciona una interfaz Windows PowerShell para vSphere API. PowerCLI incluye cmdlets para administrar los componentes de vSAN. Para obtener información sobre el uso de vSphere PowerCLI, consulte la *Documentación de vSphere PowerCLI*.

vSAN Observer

VMware vSAN Observer es una herramienta web que se ejecuta en RVC y que se utiliza para obtener análisis detallados de rendimiento y supervisión del clúster de vSAN. Utilice vSAN Observer para consultar las estadísticas de rendimiento de la capa de capacidad, la información estadística acerca de los grupos de discos físicos, la carga actual en la CPU, el consumo de los grupos de memoria de vSAN, la distribución de objetos físicos y en la memoria en clústeres de vSAN.

Para obtener información sobre la configuración, el inicio y el uso de RVC y vSAN Observer, consulte el *manual de referencia de solución de problemas de vSAN*.

vSAN y el almacenamiento tradicional

Aunque vSAN comparte muchas características con los arreglos de almacenamiento tradicionales, la función y el comportamiento general de vSAN son diferentes. Por ejemplo, vSAN solamente puede administrar y funcionar con hosts ESXi y una instancia de vSAN solo puede admitir un único clúster.

vSAN y el almacenamiento tradicional también se diferencian en los siguientes aspectos clave:

- vSAN no necesita almacenamiento en red externo para almacenar archivos de máquinas virtuales en una ubicación remota, por ejemplo, en una red de canal de fibra (Fibre Channel, FC) o en una red de área de almacenamiento (Storage Area Network, SAN).
- Con el almacenamiento tradicional, el administrador de almacenamiento asigna anticipadamente el espacio de almacenamiento en los distintos sistemas de almacenamiento. vSAN convierte de manera automática los recursos locales de almacenamiento físico de los hosts ESXi en un solo grupo de almacenamiento. Estos grupos pueden dividirse y asignarse a máquinas virtuales y aplicaciones en función de sus requisitos de calidad de servicio.
- vSAN no contempla el concepto de volúmenes de almacenamiento tradicionales basados en recursos compartidos de NFS o LUN, aunque el servicio del destino iSCSI use LUN para habilitar un iniciador en un host remoto con el objetivo de transferir datos de nivel de bloque a un dispositivo de almacenamiento del clúster de vSAN.
- Algunos protocolos de almacenamiento estándares, como FCP, no se aplican a vSAN.
- vSAN está altamente integrado con vSphere. A diferencia del almacenamiento tradicional, no se necesitan una consola de almacenamiento ni complementos dedicados para vSAN. Puede implementar, administrar y supervisar vSAN mediante vSphere Web Client.
- No se necesita un administrador de almacenamiento dedicado para administrar vSAN. En lugar de ello, un administrador de vSphere puede administrar un entorno de vSAN.
- Con el uso de vSAN, se asignan directivas de almacenamiento de máquina virtual de manera automática cuando se implementan máquinas virtuales nuevas. Es posible cambiar las directivas de almacenamiento de manera dinámica según sea necesario.

Compilar un clúster de vSAN

Si está considerando usar vSAN, puede elegir entre más de una solución de configuración para implementar un clúster de vSAN.

Según sus requisitos, puede implementar vSAN de una de las siguientes maneras:

vSAN Ready Node

vSAN Ready Node es una solución preconfigurada del software vSAN que proporcionan los partners de VMware, como Cisco, Dell, Fujitsu, IBM y Supermicro. Esta solución incluye configuración de servidores validada en un factor de forma de hardware probado y certificado para la implementación de vSAN que recomiendan el OEM del servidor y VMware. Para obtener información sobre la solución vSAN Ready Node para un partner específico, visite el sitio web de partners de VMware.

Clúster de vSAN definido por el usuario

Puede compilar un clúster de vSAN seleccionando componentes de software y hardware individuales, como los controladores, el firmware y las controladoras de E/S de almacenamiento que se enumeran en el sitio web de la Guía de compatibilidad de vSAN (VCG), en la siguiente URL:http://www.vmware.com/resources/compatibility/search.php. Puede elegir cualquier tipo de servidores, controladoras de E/S de almacenamiento, dispositivos de capacidad y dispositivos flash de almacenamiento en caché y memoria, y cualquier cantidad de núcleos que necesite por CPU, etc. que se

certifiquen y se enumeren en el sitio web de VCG. Consulte la información de compatibilidad del sitio web de VCG antes de elegir los componentes de software y hardware, los controladores, el firmware y las controladoras de E/S de almacenamiento compatibles con vSAN. Al diseñar un clúster de vSAN, use únicamente dispositivos, firmware y controladores que se enumeren en el sitio web de VCG. El uso de versiones de software y hardware no enumeradas en VCG puede ocasionar un error del clúster o una pérdida de datos inesperada. Para obtener información sobre el diseño de un clúster de vSAN, consulte Capítulo 3, "Diseñar y dimensionar un clúster de vSAN," página 21.

Integrar con otras herramientas de software de VMware

Una vez que vSAN está activo y en funcionamiento, se integra con el resto de la pila de software de VMware. Puede hacer la mayoría de las cosas que con el almacenamiento tradicional utilizando componentes y características de vSphere, que incluyen vSphere vMotion, instantáneas, clones, Distributed Resource Scheduler (DRS), vSphere High Availability, vCenter Site Recovery Manager y más.

Integrar con vSphere HA

Puede habilitar vSphere HA y vSAN en el mismo clúster. Al igual que con los almacenes de datos tradicionales, vSphere HA proporciona el mismo nivel de protección para las máquinas virtuales en los almacenes de datos de vSAN. El nivel de protección impone restricciones específicas cuando interactúan vSphere HA y vSAN . Para obtener información sobre consideraciones específicas relacionadas con la integración de vSphere HA y vSAN, consulte "Usar vSAN y vSphere HA," página 56.

Integrar con VMware Horizon View

Puede integrar vSAN con VMware Horizon View. Cuando se integra, vSAN proporciona los siguientes beneficios a los entornos de escritorios virtuales:

- Almacenamiento de alto rendimiento con almacenamiento en caché automático
- Administración de almacenamiento basada en directivas, para corrección automática

Para obtener información sobre la integración de vSAN con VMware Horizon, consulte el documento *VMware Horizon with View*. Si desea información sobre el diseño y el dimensionamiento de VMware Horizon View para vSAN, consulte la *guía de diseño y dimensionamiento para Horizon View*.

Limitaciones de vSAN

En este tema se analizan las limitaciones de vSAN.

Al trabajar con vSAN, tenga en cuenta las siguientes limitaciones:

- vSAN no admite hosts que participen en varios clústeres de vSAN. Sin embargo, un host de vSAN puede acceder a otros recursos de almacenamiento externo que se comparten entre todos los clústeres.
- vSAN no admite vSphere DPM ni Storage I/O Control.
- vSAN no admite reservas SCSI.
- vSAN no admite RDM, VMFS, partición de diagnóstico ni otras características de acceso a dispositivos.

Requisitos para habilitar vSAN 2

Antes de activar vSAN, compruebe que el entorno cumpla todos los requisitos.

Este capítulo cubre los siguientes temas:

Requisitos de hardware para vSAN

Compruebe que los hosts ESXi de su organización cumplan con los requisitos de hardware de vSAN.

Requisitos de dispositivos de almacenamiento

Todos los dispositivos de capacidad, los controladores y las versiones de firmware de la configuración de vSAN deben estar certificados y enumerarse en la sección vSAN de la *Guía de compatibilidad de VMware*.

Tabla 2-1. Requisitos de dispositivos de almacenamiento para hosts de vSAN

Componente de almacenamiento	Requisitos
Memoria caché	■ Un dispositivo flash PCIe o un disco de estado sólido (SSD) SAS o SATA. ■ Antes de calcular el atributo **Primary level of failures to tolerate** (Nivel principal de errores que se toleran), compruebe el tamaño del dispositivo flash de almacenamiento en caché en cada grupo de discos. Compruebe que este dispositivo proporcione, al menos, el 10 % del almacenamiento que se espera que se consuma en los dispositivos de capacidad, sin incluir réplicas, como los duplicados. ■ vSphere Flash Read Cache no debe usar ninguno de los dispositivos flash reservados para la memoria caché de vSAN. ■ No se debe aplicar formato con VMFS u otro sistema de archivos a los dispositivos flash de memoria caché.
Almacenamiento de datos de máquinas virtuales	■ Para la configuración de grupos híbridos, asegúrese de que haya, al menos, un disco magnético SATA, SAS o SAS NL disponible. ■ Para la configuración híbrida de grupos basados íntegramente en tecnología flash, asegúrese de que haya, al menos, un dispositivo flash PCIe o un disco de estado sólido SAS o SATA.
Controladoras de almacenamiento	Un adaptador de bus de host (HBA) SAS o SATA o una controladora RAID que esté en modo de acceso directo o RAID 0.

Memoria

Los requisitos de memoria de vSAN dependen de la cantidad de dispositivos y grupos de discos que debe administrar el hipervisor de ESXi. Cada host debe contener, como mínimo, 32 GB de memoria para admitir la cantidad máxima de grupos de discos (5) y de dispositivos de capacidad por cada grupo de discos (7).

Dispositivos flash de arranque

Durante la instalación, el instalador de ESXi crea una partición de volcado de núcleo en el dispositivo de arranque. El tamaño predeterminado de esta partición cumple con la mayoría de los requisitos de instalación.

- Si la memoria del host ESXi es de 512 GB o menos, puede arrancar el host desde un dispositivo USB, SD o SATADOM. Al arrancar un host vSAN desde un dispositivo USB o una tarjeta SD, el tamaño del dispositivo de arranque debe ser de 4 GB como mínimo.
- Si la memoria del host ESXi supera los 512 GB, debe arrancar el host desde un dispositivo de disco o SATADOM. Al arrancar un host de vSAN desde un dispositivo SATADOM, debe usar un dispositivo de celdas de un solo nivel (single-level cell, SLC). El tamaño del dispositivo de arranque debe ser de 16 GB como mínimo.

NOTA: vSAN 6.5 y versiones posteriores permiten cambiar el tamaño de una partición de volcado de núcleo existente en un host ESXi de un clúster de vSAN, por lo que es posible arrancar desde dispositivos USB/SD. Para obtener más información, consulte el artículo de la base de conocimientos de VMware en http://kb.vmware.com/kb/2147881.

Al arrancar un host ESXi 6.0 o posterior desde un dispositivo USB o una tarjeta SD, los registros de seguimiento de vSAN se escriben en el disco RAM. Estos registros se descargan de forma automática en medios persistentes durante el apagado o el bloqueo del sistema (estado de alerta). Este es el único método admitido para controlar los rastros de vSAN al arrancar una instancia de ESXi desde un dispositivo USB o una tarjeta SD. Si se producen cortes de energía, los registros de seguimiento de vSAN no se conservan.

Al arrancar un host ESXi 6.0 o posterior desde un dispositivo SATADOM, los registros de seguimiento de vSAN se escriben directamente en el dispositivo SATADOM. Por lo tanto, es importante que el dispositivo SATADOM cumpla con las especificaciones que se detallan en esta guía.

Requisitos de clúster para vSAN

Compruebe que un clúster de host cumpla con los requisitos para habilitar vSAN.

- Todos los dispositivos de capacidad, los controladores y las versiones de firmware de la configuración de vSAN deben estar certificados y enumerarse en la sección vSAN de la *Guía de compatibilidad de VMware*.
- Un clúster de vSAN debe tener, como mínimo, tres hosts que aporten capacidad al clúster. Para obtener información sobre las consideraciones asociadas con un clúster de tres hosts, consulte "Consideraciones de diseño para un clúster de vSAN," página 30.
- Un host que reside en un clúster de vSAN no debe participar en otros clústeres.

Requisitos de software para vSAN

Compruebe que los componentes de vSphere en su entorno cumplan con los requisitos de la versión de software para usar vSAN.

Para usar el conjunto completo de funcionalidades de vSAN, los hosts ESXi que participan en clústeres de vSAN deben ser de la versión 6.5 o posteriores. Durante la actualización de vSAN desde versiones anteriores, puede conservar la versión de formato en disco actual, pero, en tal caso, no podrá utilizar muchas de las nuevas funciones. El software de vSAN 6.6 y versiones posteriores admiten todos los formatos en disco.

Requisitos de red para vSAN

Compruebe que la infraestructura de red y la configuración de red de los hosts ESXi cumplan con los requisitos de red mínimos para vSAN.

Tabla 2-2. Requisitos de red para vSAN

Componente de red	Requisito
Ancho de banda de hosts	Cada host debe tener un ancho de banda mínimo dedicado para vSAN. ■ Ancho de banda dedicado de 1 Gbps para configuraciones híbridas ■ Ancho de banda dedicado o compartido de 10 Gbps para configuraciones basadas íntegramente en tecnología flash Para obtener información sobre de las consideraciones de red de vSAN, consulte "Diseñar la red de vSAN," página 31.
Conexión entre hosts	Cada host del clúster de vSAN, independientemente de si aporta capacidad o no, debe contar con un adaptador de red de VMkernel para el tráfico de vSAN. Consulte "Configurar una red de VMkernel para vSAN," página 50.
Red de hosts	Todos los hosts del clúster de vSAN deben estar conectados a una red de capa 2 o capa 3 de vSAN.
Compatibilidad con IPv4 e IPv6	La red de vSAN es compatible con IPv4 e IPv6.

Requisitos de licencia

Compruebe que tenga una licencia para vSAN.

El uso de vSAN en entornos de producción requiere una licencia especial que debe asignar a los clústeres de vSAN.

Puede asignar una licencia de vSAN estándar al clúster o una licencia que abarque funciones avanzadas. Las características avanzadas incluyen codificación de borrado RAID 5/6 y desduplicación y compresión. Los límites de E/S por segundo y los clústeres ampliados requieren una licencia empresarial. Para obtener más información sobre la asignación de licencias, consulte "Configurar los ajustes de licencia para un clúster de vSAN," página 54.

La capacidad de la licencia debe cubrir la cantidad total de CPU del clúster.

Diseñar y dimensionar un clúster de vSAN

3

Para un mejor rendimiento y uso, planifique las capacidades y la configuración de los hosts y sus dispositivos de almacenamiento antes de implementar vSAN en un entorno de vSphere. Evalúe detenidamente ciertas configuraciones de red y de host dentro del clúster de vSAN.

El documento *Administrar VMware vSAN* examina puntos clave sobre el diseño y el dimensionamiento de un clúster de vSAN. Para obtener instrucciones detalladas sobre el diseño y el dimensionamiento de un clúster de vSAN, consulte *Guía de diseño y dimensionamiento de VMware vSAN*.

Este capítulo cubre los siguientes temas:

Diseñar y dimensionar componentes de almacenamiento de vSAN

Planifique la capacidad y la memoria caché en función del consumo esperado. Tenga en cuenta los requisitos de disponibilidad y resistencia.

- Planificar la capacidad en vSAN página 22

  Puede dimensionar la capacidad de un almacén de datos de vSAN para alojar los archivos de las máquinas virtuales (VM) en el clúster y para controlar los errores en las operaciones de mantenimiento.

- Consideraciones de diseño para dispositivos flash de almacenamiento en caché en vSAN página 24

  Planifique la configuración de dispositivos flash para la capacidad basada íntegramente en tecnología flash y la memoria caché de vSAN a fin de proporcionar alto rendimiento y el espacio de almacenamiento necesario, además de adaptarse al crecimiento futuro.

- Consideraciones de diseño para dispositivos de capacidad en vSAN página 27

  Planifique la configuración de dispositivos de capacidad para configuraciones basadas íntegramente en tecnología flash de vSAN a fin de proporcionar alto rendimiento y el espacio de almacenamiento necesario, además de adaptarse al crecimiento futuro.

-

  Planifique la cantidad y el tamaño de los discos magnéticos para la capacidad en las configuraciones híbridas en función de los requisitos de rendimiento y espacio de almacenamiento.

-

  Incluya las controladoras de almacenamiento en los hosts de un clúster de vSAN que mejor se adecuen a los requisitos de rendimiento y disponibilidad.

Planificar la capacidad en vSAN

Puede dimensionar la capacidad de un almacén de datos de vSAN para alojar los archivos de las máquinas virtuales (VM) en el clúster y para controlar los errores en las operaciones de mantenimiento.

Capacidad en bruto

Para determinar la capacidad en bruto de un almacén de datos de vSAN, multiplique la cantidad total de grupos de discos del clúster por el tamaño de los dispositivos de capacidad de dichos grupos de discos y, a continuación, reste la sobrecarga requerida por el formato en disco de vSAN.

Nivel principal de errores que se toleran

Al planificar la capacidad del almacén de datos de vSAN, independientemente de la cantidad de máquinas virtuales y el tamaño de los archivos de VMDK, debe tener en cuenta los atributos **Nivel primario de errores que se toleran** y **Método de tolerancia a errores** de las directivas de almacenamiento de las máquinas virtuales del clúster.

Nivel primario de errores que se toleran desempeña una función importante al planificar y dimensionar la capacidad de almacenamiento de vSAN. Según los requisitos de disponibilidad de una máquina virtual, la configuración puede producir un consumo duplicado o más en comparación con el consumo de una máquina virtual y los dispositivos individuales.

Por ejemplo, si **Failure tolerance method** (Método de tolerancia a errores) se establece en **RAID-1 (Mirroring) - Performance** (RAID-1 [reflejo]: rendimiento) y **Primary level of failures to tolerate** (Nivel principal de errores que se toleran) o PFTT se establece en 1, las máquinas virtuales pueden utilizar aproximadamente un 50 % de la capacidad en bruto. Si el PFTT se establece en 2, la capacidad utilizable es aproximadamente de un 33 %. Si el PFTT se establece en 3, la capacidad utilizable es aproximadamente de un 25 %.

Sin embargo, si **Failure tolerance method** (Método de tolerancia a errores) se establece en **RAID-5/6 (Erasure Coding) - Capacity** (RAID-5/6 [codificación de borrado]: capacidad) y el PFTT se establece en 1, las máquinas virtuales pueden utilizar aproximadamente un 75 % de la capacidad en bruto. Si el PFTT se establece en 2, la capacidad utilizable es aproximadamente de un 67 %. Para obtener más información sobre RAID 5/6, consulte "Usar la codificación de borrado RAID 5 o RAID 6," página 80.

Para obtener información sobre los atributos de una directiva de almacenamiento de vSAN, consulte Capítulo 12, "Usar las directivas de vSAN," página 135.

Calcular la capacidad necesaria

Planifique la capacidad requerida para las máquinas virtuales en un clúster con el reflejo RAID 1 de acuerdo con los siguientes criterios:

1 Calcule el espacio de almacenamiento que se espera que consuman las máquinas virtuales del clúster de vSAN.

```
expected overall consumption = number of VMs in the cluster * expected percentage of
consumption per VMDK
```

2 Tenga en cuenta el atributo **Primary level of failures to tolerate** (Nivel principal de errores que se toleran) configurado en las directivas de almacenamiento para las máquinas virtuales del clúster. Este atributo tiene un impacto directo en la cantidad de réplicas de un archivo VMDK en los hosts del clúster.

```
datastore capacity = expected overall consumption * (PFTT + 1)
```

3 Estime el requisito de sobrecarga del formato en disco de vSAN.

- El formato en disco versión 3.0 y posteriores agrega una sobrecarga adicional, que generalmente no excede el 1-2 % de capacidad por dispositivo. La desduplicación y la compresión con la suma de comprobación de software habilitada requieren una sobrecarga adicional de aproximadamente 6,2 % de capacidad por dispositivo.
- El formato en disco versión 2.0 agrega una sobrecarga adicional, que generalmente no excede el 1-2 % de capacidad por dispositivo.
- El formato en disco versión 1.0 agrega una sobrecarga adicional de aproximadamente 1 GB por dispositivo de capacidad.

Directrices para el dimensionamiento de la capacidad

- Deje al menos un 30 % de espacio sin utilizar para impedir que vSAN redistribuya la carga de almacenamiento. vSAN redistribuye los componentes en el clúster cuando el consumo de un solo dispositivo de capacidad alcanza el 80 % o más. La operación de redistribución puede afectar el rendimiento de las aplicaciones. Para evitar estos problemas, mantenga el consumo de almacenamiento en un nivel inferior al 70 %.
- Planifique capacidad adicional para controlar posibles errores o reemplazos de los dispositivos de capacidad, los grupos de discos y los hosts. Cuando un dispositivo de capacidad no está accesible, vSAN recupera los componentes desde otro dispositivo del clúster. Cuando un dispositivo de memoria caché flash experimenta un error o se quita, vSAN recupera los componentes de todo el grupo de discos.
- Reserve capacidad adicional para garantizar que vSAN recupere componentes después de un error de host o cuando un host entre en modo de mantenimiento. Por ejemplo, aprovisione hosts de modo que quede capacidad libre suficiente para que los componentes se reconstruyan correctamente después de un error de un host o durante el mantenimiento. Esto es importante cuando existen más de tres hosts, a fin de tener suficiente espacio libre para reconstruir los componentes con errores. Si un host tiene errores, la reconstrucción se realiza en el almacenamiento disponible en el otro host y, de esta forma, se puede tolerar otro error. No obstante, en un clúster de tres hosts, vSAN no ejecuta la operación de recompilación si el parámetro **Nivel primario de errores que se toleran** está establecido como 1 porque, cuando se produce un error en un host, solo quedan dos hosts en el clúster. Para tolerar una reconstrucción después de un error, debe contar con, al menos, tres hosts.
- Proporcione suficiente espacio de almacenamiento temporal para los cambios en la directiva de almacenamiento de máquina virtual de vSAN. Al cambiar de manera dinámica una directiva de almacenamiento de máquina virtual, es posible que vSAN cree una distribución de las réplicas que conforman un objeto. Cuando vSAN crea instancias de esas réplicas y las sincroniza con la réplica original, el clúster debe proporcionar espacio adicional temporal.
- Si planifica utilizar las características avanzadas, como la suma de comprobación de software o la desduplicación y la compresión, reserve capacidad adicional para controlar la sobrecarga operativa.

Consideraciones sobre los objetos de máquinas virtuales

Cuando planifique la capacidad de almacenamiento del almacén de datos de vSAN, considere el espacio requerido en el almacén de datos para los objetos del espacio de nombres del directorio principal de la máquina virtual, las instantáneas y los archivos de intercambio.

- Espacio de nombres del directorio principal de la máquina virtual. Puede asignar una directiva de almacenamiento específicamente para el espacio de nombres del directorio principal de una máquina virtual. Para prevenir una asignación innecesaria de capacidad y memoria caché, vSAN aplica solamente la configuración de **Nivel primario de errores que se toleran** y **Forzar aprovisionamiento** desde la directiva del espacio de nombres del directorio principal de la máquina virtual. Planifique el espacio de almacenamiento para cumplir con los requisitos de una directiva de almacenamiento asignada a un espacio de nombres del directorio principal de la máquina virtual cuyo valor de **Primary level of failures to tolerate** (Nivel principal de errores que se toleran) sea mayor que 0.
- Instantáneas. Los dispositivos delta heredan la directiva del archivo de VMDK de base. Planifique espacio adicional de acuerdo con los valores esperados de tamaño y cantidad de instantáneas, y de acuerdo con la configuración de las directivas de almacenamiento de vSAN.

  Es posible que el espacio requerido sea diferente. El tamaño depende de la frecuencia con la que la máquina virtual cambia datos y del tiempo que una instantánea permanece asociada a la máquina virtual.
- Archivos de intercambio. vSAN usa una directiva de almacenamiento individual para los archivos de intercambio de las máquinas virtuales. La directiva tolera un solo error, define ausencia de fraccionamiento y reserva de memoria caché de lectura, y permite el aprovisionamiento forzado.

Consideraciones de diseño para dispositivos flash de almacenamiento en caché en vSAN

Planifique la configuración de dispositivos flash para la capacidad basada íntegramente en tecnología flash y la memoria caché de vSAN a fin de proporcionar alto rendimiento y el espacio de almacenamiento necesario, además de adaptarse al crecimiento futuro.

Elegir entre dispositivos flash PCIe o SSD

Elija dispositivos flash PCIe o SSD en función de los requisitos de rendimiento, capacidad, resistencia de escritura y costo del almacenamiento de vSAN.

- Compatibilidad. El modelo de los dispositivos PCIe o SSD debe enumerarse en la sección vSAN de la *Guía de compatibilidad de VMware*.
- Rendimiento. Los dispositivos PCIe tienen, por lo general, un rendimiento más rápido que los dispositivos SSD.
- Capacidad. La capacidad máxima que está disponible para dispositivos PCIe, por lo general, es mayor que la capacidad máxima que se muestra actualmente para los dispositivos SSD para vSAN en la *Guía de compatibilidad de VMware*.
- Resistencia de escritura. La resistencia de escritura de los dispositivos PCIe o SSD debe cumplir con los requisitos de capacidad o memoria caché en las configuraciones basadas íntegramente en tecnología flash y con los requisitos de memoria caché en las configuraciones híbridas.

  Para obtener información sobre los requisitos de resistencia de escritura para las configuraciones híbridas y basadas íntegramente en tecnología flash, consulte la *Guía de diseño y dimensionamiento de VMware vSAN*. Para obtener información sobre la clase de resistencia de escritura de los dispositivos PCIe y SSD, consulte la sección vSAN de la *Guía de compatibilidad de VMware*.
- Costo. Los dispositivos PCIe tienen, por lo general, un costo más alto que los dispositivos SSD.

Dispositivos Flash como memoria caché de vSAN

Diseñe la configuración de la memoria caché flash de vSAN para cumplir con los requisitos de resistencia de escritura, rendimiento y crecimiento potencial en función de estas consideraciones.

Tabla 3-1. Dimensionar la memoria caché de vSAN

<table>
<tr><th>Configuración de almacenamiento</th><th>Consideraciones</th></tr>
<tr><td>Configuraciones híbridas y basadas íntegramente en tecnología flash</td><td>El dispositivo flash de almacenamiento en caché debe proporcionar, al menos, el 10 % del almacenamiento que se espera que se consuma en las máquinas virtuales, sin incluir réplicas, como los duplicados.

El atributo Primary level of failures to tolerate (Nivel principal de errores que se toleran) de la directiva de almacenamiento de máquina virtual no afecta el tamaño de la memoria caché.
Una proporción más alta entre la memoria caché y la capacidad facilita el crecimiento futuro de la capacidad. El sobredimensionamiento de la memoria caché le permite agregar más capacidad a un grupo de discos existente sin necesidad de aumentar el tamaño de la memoria caché.
Los dispositivos flash de almacenamiento en caché deben tener una mayor resistencia de escritura.
Cuando un dispositivo flash de almacenamiento en caché alcanza el fin de su vida útil, reemplazarlo es más complicado que reemplazar un dispositivo de capacidad porque esta operación afecta a todo el grupo de discos.
Si agrega más dispositivos flash con la finalidad de aumentar el tamaño de la memoria caché, debe crear más grupos de discos. La proporción entre dispositivos flash de almacenamiento en caché y grupos de discos siempre es 1:1.

Una configuración de varios grupos de discos proporciona las siguientes ventajas:
Menor riesgo de fallo porque habrá menos dispositivos de capacidad afectados si un dispositivo de almacenamiento en caché falla.
Rendimiento potencialmente mejorado si se implementan varios grupos de discos que contengan dispositivos flash de almacenamiento en caché más pequeños.
No obstante, cuando se configuran varios grupos de discos, aumenta el consumo de memoria de los hosts.</td></tr>
<tr><td>Configuraciones basadas íntegramente en tecnología flash</td><td>En las configuraciones basadas íntegramente en tecnología flash, vSAN usa la capa de memoria caché únicamente para el almacenamiento en caché de escritura. La memoria caché de escritura debe poder controlar una gran cantidad de actividades de escritura. Este enfoque prolonga la vida útil de la tecnología flash de capacidad que puede ser menos costosa y puede tener una menor resistencia de escritura.</td></tr>
<tr><td>Configuraciones híbridas</td><td>Si, por motivos de rendimiento, se configura la reserva de memoria caché de lectura en la directiva de almacenamiento de máquina virtual activa, los hosts del clúster de vSAN deben tener suficiente memoria caché para satisfacer la reserva durante una operación de mantenimiento o de recompilación posterior a un error.

Si la memoria caché de lectura disponible no es suficiente para satisfacer la reserva, se produce un error en la operación de mantenimiento o de reconstrucción. Use la reserva de memoria caché de lectura solamente si debe cumplir un requisito de rendimiento específico conocido para una carga de trabajo en particular.

El uso de instantáneas consume recursos de memoria caché. Si tiene pensado usar varias instantáneas, considere la posibilidad de dedicar más memoria caché que la proporción convencional del 10 % entre la capacidad de memoria caché y la capacidad utilizada.</td></tr>
</table>

Consideraciones de diseño para dispositivos de capacidad en vSAN

Planifique la configuración de dispositivos de capacidad para configuraciones basadas íntegramente en tecnología flash de vSAN a fin de proporcionar alto rendimiento y el espacio de almacenamiento necesario, además de adaptarse al crecimiento futuro.

Elegir entre dispositivos flash PCIe o SSD

Elija dispositivos flash PCIe o SSD en función de los requisitos de rendimiento, capacidad, resistencia de escritura y costo del almacenamiento de vSAN.

- Compatibilidad. El modelo de los dispositivos PCIe o SSD debe enumerarse en la sección vSAN de la *Guía de compatibilidad de VMware*.
- Rendimiento. Los dispositivos PCIe tienen, por lo general, un rendimiento más rápido que los dispositivos SSD.
- Capacidad. La capacidad máxima que está disponible para dispositivos PCIe, por lo general, es mayor que la capacidad máxima que se muestra actualmente para los dispositivos SSD para vSAN en la *Guía de compatibilidad de VMware*.
- Resistencia de escritura. La resistencia de escritura de los dispositivos PCIe o SSD debe cumplir con los requisitos de capacidad o memoria caché en las configuraciones basadas íntegramente en tecnología flash y con los requisitos de memoria caché en las configuraciones híbridas.

  Para obtener información sobre los requisitos de resistencia de escritura para las configuraciones híbridas y basadas íntegramente en tecnología flash, consulte la *Guía de diseño y dimensionamiento de VMware vSAN*. Para obtener información sobre la clase de resistencia de escritura de los dispositivos PCIe y SSD, consulte la sección vSAN de la *Guía de compatibilidad de VMware*.
- Costo. Los dispositivos PCIe tienen, por lo general, un costo más alto que los dispositivos SSD.

Dispositivos Flash como capacidad de vSAN

En las configuraciones basadas íntegramente en tecnología flash, vSAN no usa memoria caché para las operaciones de lectura y no aplica el ajuste de configuración de reserva de memoria caché de lectura establecido en la directiva de almacenamiento de máquina virtual. Para la memoria caché, puede usar una pequeña cantidad de dispositivos flash más costosos que ofrecen alta resistencia de escritura. Para la capacidad, puede usar dispositivos flash, que son menos costosos y ofrecen una menor resistencia de escritura.

Planifique una configuración de dispositivos de capacidad flash siguiendo estas directrices:

- Para obtener un mejor rendimiento de vSAN, use más grupos de discos de dispositivos de capacidad flash más pequeños.
- Para obtener un rendimiento equilibrado y previsible, use dispositivos de capacidad flash del mismo tipo y modelo.

Consideraciones de diseño para discos magnéticos en vSAN

Planifique la cantidad y el tamaño de los discos magnéticos para la capacidad en las configuraciones híbridas en función de los requisitos de rendimiento y espacio de almacenamiento.

Dispositivos magnéticos SAS, SAS NL y SATA

Use dispositivos magnéticos SAS, SAS NL o SATA en función de los requisitos de rendimiento, capacidad y costo del almacenamiento de vSAN.

- Compatibilidad. El modelo del disco magnético debe estar certificado y aparecer en la sección vSAN de la *Guía de compatibilidad de VMware*.

- Rendimiento. Los dispositivos SAS y SAS NL ofrecen un rendimiento más rápido que los discos SATA.
- Capacidad. La capacidad de los discos magnéticos SAS, SAS NL y SATA para vSAN está disponible en la sección vSAN de la *Guía de compatibilidad de VMware*. Considere la posibilidad de usar una mayor cantidad de dispositivos más pequeños en lugar de una menor cantidad de dispositivos más grandes.
- Costo. Los dispositivos SAS y SAS NL son más costosos que los discos SATA.

El uso de discos SATA en lugar de dispositivos SAS y SAS NL se justifica en los entornos en los que la capacidad y la reducción del costo tienen una prioridad mayor que el rendimiento.

Discos magnéticos como capacidad de vSAN

Planifique una configuración de discos magnéticos siguiendo estas directrices:

- Para obtener un mejor rendimiento de vSAN, use una gran cantidad de discos magnéticos de menor capacidad.

  Debe contar con suficientes discos magnéticos para proporcionar un rendimiento agregado adecuado para la transferencia de datos entre dispositivos de memoria caché y de capacidad. El uso de una mayor cantidad de dispositivos pequeños proporciona un mejor rendimiento que el uso de una menor cantidad de dispositivos grandes. El uso de varios ejes de discos magnéticos puede agilizar el proceso de descarga.

  En los entornos con muchas máquinas virtuales, la cantidad de discos magnéticos también es importante para las operaciones de lectura cuando no hay datos disponibles en la memoria caché de lectura y vSAN lee los datos del disco magnético. En los entornos con una pequeña cantidad de máquinas virtuales, la cantidad de discos incide en las operaciones de lectura si **Number of disk stripes per object** (Cantidad de fracciones de discos por objeto) en la directiva de almacenamiento de máquina virtual activa es mayor que uno.
- Para obtener un rendimiento equilibrado y previsible, use discos magnéticos del mismo tipo y modelo en un almacén de datos de vSAN.
- Dedique una alta cantidad de discos magnéticos para cumplir con el valor de los atributos **Primary level of failures to tolerate** (Nivel principal de errores que se toleran) y **Number of disk stripes per object** (Cantidad de fracciones de discos por objeto) en las directivas de almacenamiento definidas. Si desea obtener información sobre el uso de directivas de almacenamiento de máquina virtual para vSAN, consulte Capítulo 12, "Usar las directivas de vSAN," página 135.

Consideraciones de diseño para las controladoras de almacenamiento en vSAN

Incluya las controladoras de almacenamiento en los hosts de un clúster de vSAN que mejor se adecuen a los requisitos de rendimiento y disponibilidad.

- Use los modelos de las controladoras de almacenamiento y las versiones de firmware y controladores que se enumeran en la *Guía de compatibilidad de VMware*. Busque vSAN en la *Guía de compatibilidad de VMware*.
- De ser posible, use varias controladoras de almacenamiento, a fin de mejorar el rendimiento y aislar un error potencial de una controladora y circunscribirlo a un solo subconjunto de grupos de discos.
- Use las controladoras de almacenamiento que ofrezcan la profundidad de cola más alta en la *Guía de compatibilidad de VMware*. El uso de controladoras con colas de gran profundidad mejora el rendimiento. Por ejemplo, cuando vSAN recompila componentes después de un error o cuando un host entra en modo de mantenimiento.
- Use las controladoras de almacenamiento en modo de acceso directo para obtener el mejor rendimiento de vSAN. Las controladoras de almacenamiento en modo de RAID 0 requieren mayores esfuerzos de configuración y mantenimiento que las controladoras de almacenamiento en modo de acceso directo.

Diseñar y dimensionar hosts de vSAN

Planifique la configuración de los hosts en el clúster de vSAN para obtener los mejores niveles de rendimiento y disponibilidad.

Memoria y CPU

Tamaño de la memoria y la CPU de los hosts en el clúster de vSAN en función de las siguientes consideraciones.

Tabla 3-2. Dimensionar la memoria y CPU de los hosts de vSAN

Compute Resource (Recurso informático)	Consideraciones
Memoria	■ Memoria por máquina virtual ■ Memoria por host en función de la cantidad esperada de máquinas virtuales ■ Al menos 32 GB de memoria para vSAN completamente operativo con 5 grupos de discos por host y 7 dispositivos de capacidad por grupo de discos Los hosts con una memoria de 512 GB o menos pueden arrancar desde un dispositivo USB, SD o SATADOM. Si la memoria del host supera los 512 GB, arranque el host desde un dispositivo de disco o SATADOM.
CPU	■ Ranuras por host ■ Núcleos por ranura ■ Cantidad de vCPU en función de la cantidad esperada de máquinas virtuales ■ Proporción entre vCPU y núcleos ■ Sobrecarga de CPU del 10 % para vSAN

Redes de hosts

Proporcione más ancho de banda para el tráfico de vSAN a fin de mejorar el rendimiento.

- Si tiene planificado usar hosts con adaptadores 1 GbE, dedique adaptadores para vSAN únicamente. Para las configuraciones basadas íntegramente en tecnología flash, planifique hosts que tengan adaptadores 10 GbE dedicados o compartidos.
- Si tiene planificado usar adaptadores 10 GbE, pueden compartirse con otros tipos de tráfico para configuraciones híbridas y basadas íntegramente en tecnología flash.
- Si un adaptador 10 GbE se comparte con otros tipos de tráfico, use vSphere Distributed Switch para el tráfico de vSAN a fin de aislar el tráfico mediante Network I/O Control y VLAN.
- Cree un grupo de adaptadores físicos para el tráfico de vSAN a fin de obtener redundancia.

Varios grupos de discos

Si la memoria caché flash o la controladora de almacenamiento deja de responder, un grupo de discos completo puede fallar. Como consecuencia, vSAN recompila todos los componentes del grupo de discos con errores en otra ubicación del clúster.

Si se utilizan varios grupos de discos, y cada uno de ellos proporciona menos capacidad, se obtienen los siguientes beneficios y desventajas:

- Beneficios
  - El rendimiento mejora debido a que el almacén de datos tiene más memoria caché agregada y las operaciones de E/S son más rápidas.

- El riesgo de error se reparte entre varios grupos de discos.
- Si se produce un error en un grupo de discos, vSAN recompila menos componentes, por lo que mejora el rendimiento.

- Desventajas
  - Los costes aumentan porque se necesitan dos o más dispositivos de almacenamiento en caché.
  - Se precisa más memoria para gestionar más grupos de discos.
  - Se necesitan varias controladoras de almacenamiento para reducir el riesgo de tener un único punto de error.

Bahías de unidades

A fin de facilitar las tareas de mantenimiento, considere usar hosts cuyas bahías de unidades y ranuras PCIe se encuentren en la parte frontal del cuerpo del servidor.

Servidores blade y almacenamiento externo

Por lo general, la capacidad de los servidores blade no escala en un almacén de datos de vSAN porque cuentan con una cantidad limitada de ranuras de discos. Para ampliar la capacidad planificada de servidores blade, use gabinetes de almacenamiento externos. Para obtener información sobre los modelos compatibles de gabinetes de almacenamiento externos, consulte la *Guía de compatibilidad de VMware*.

Conectar e intercambiar dispositivos en caliente

Tenga en cuenta la compatibilidad con el modo de acceso directo a la controladora de almacenamiento para facilitar la conexión y la sustitución en caliente de los discos magnéticos y los dispositivos de capacidad flash en un host. Si una controladora funciona en modo RAID 0, deberá realizar pasos adicionales antes de que el host pueda detectar la unidad nueva.

Consideraciones de diseño para un clúster de vSAN

Diseñe la configuración de los hosts y los nodos de administración para obtener los mejores niveles de disponibilidad y tolerancia al crecimiento del consumo.

Dimensionar el clúster de vSAN en función de los errores que se deben tolerar

Debe configurar el atributo **Primary level of failures to tolerate** (Nivel principal de errores que se toleran) o PFTT en las directivas de almacenamiento de máquina virtual para controlar los errores de los hosts. La cantidad de hosts requeridos para el clúster se calcula de la siguiente manera: `2 * PFTT + 1`. Cuantos más errores se configura el clúster para tolerar, mayor será la capacidad requerida.

Si los hosts del clúster están conectados en servidores de bastidor, puede organizar los hosts en dominios de errores para mejorar la administración de errores. Consulte "Diseñar y dimensionar dominios de errores de vSAN," página 34.

Limitaciones de una configuración de clúster de dos o tres hosts

En una configuración de dos o tres hosts, puede tolerar solo la falla de un host al establecer el atributo **Primary level of failures to tolerate** (Nivel principal de errores que se toleran) en 1. vSAN almacena cada una de las dos réplicas requeridas de los datos de las máquinas virtuales en hosts por separado. El objeto testigo se ubica en el tercer host. Debido a la menor cantidad de hosts en el clúster, existen las siguientes limitaciones:

- Cuando se produce un error en un host, vSAN no puede volver a compilar los datos en otro host para protegerse contra otro error.

- Si un host debe entrar en modo de mantenimiento, vSAN no puede volver a proteger los datos evacuados. Los datos quedan expuestos a un posible error mientras el host está en modo de mantenimiento.

  Solo puede utilizar la opción de evacuación de datos **Ensure data accessibility** (Garantizar accesibilidad a los datos). La opción **Evacuate all data** (Evacuar todos los datos) no está disponible, ya que el clúster no tiene un host de reserva que pueda usar para evacuar datos.

  Como consecuencia, las máquinas virtuales quedan expuestas a riesgos, ya que no estarán accesibles si se produce otro error.

Configuración de clúster equilibrada y desequilibrada

vSAN funciona mejor en hosts con configuraciones uniformes.

Utilizar hosts con diferentes configuraciones tiene las siguientes desventajas en un clúster de vSAN:

- Menor previsibilidad del rendimiento del almacenamiento, ya que vSAN no almacena la misma cantidad de componentes en cada host.
- Diferentes procedimientos de mantenimiento.
- Reducción del rendimiento en los hosts del clúster que tienen tipos más pequeños o diferentes de dispositivos de memoria caché.

Implementar vCenter Server en vSAN

Si implementa vCenter Server en el almacén de datos de vSAN, tal vez no pueda usar vCenter Server para la solución de problemas en caso de que se produzca un problema en el clúster de vSAN.

Diseñar la red de vSAN

Tenga en cuenta las características de red que pueden proporcionar disponibilidad, seguridad y ancho de banda garantizado en un clúster de vSAN.

Para obtener detalles sobre la configuración de red de vSAN, consulte *Guía de diseño y dimensionamiento de VMware vSAN* y *Guía de diseño de red de vSAN*.

Conmutación por error y equilibrio de carga de red

vSAN utiliza la directiva de formación de equipos y conmutación por error que está configurada en el conmutador virtual de respaldo solamente para redundancia de red. vSAN no utiliza la formación de equipos de NIC para el equilibrio de carga.

Si tiene planificado configurar un equipo de NIC para obtener disponibilidad, tenga en cuenta estas configuraciones de conmutación por error.

Algoritmo de formación de equipos	Configuración de conmutación por error de los adaptadores del equipo
Enrutar según el puerto virtual de origen	Activa/pasiva
Route based on IP hash (Enrutar según el hash de IP)	Activa/activa con EtherChannel estático para conmutador estándar y canal de puerto LACP para conmutador distribuido
Enrutar según carga de adaptador de red físico	Activa/activa

vSAN admite equilibrio de carga para hash de IP, pero no puede garantizar una mejora en el rendimiento para todas las configuraciones. Puede beneficiarse del hash de IP cuando vSAN se encuentra entre su gran cantidad de consumidores. En este caso, el hash de IP realiza el equilibrio de carga. Si vSAN es el único consumidor, es posible que no note ninguna mejora. Este comportamiento se aplica específicamente a los entornos 1 GbE. Por ejemplo, si usa cuatro adaptadores físicos 1 GbE con hash de IP para vSAN, es posible que no pueda aprovechar más de 1 Gbps. Este comportamiento se aplica también a todas las directivas de formación de equipos de NIC que son compatibles con VMware.

Usar unidifusión en una red de vSAN

En vSAN 6.6 y las versiones posteriores, no se requiere multidifusión en los conmutadores físicos que admiten el clúster de vSAN. Es posible designar una red de unidifusión simple para vSAN. Las versiones anteriores de vSAN dependen de la multidifusión para habilitar el latido y para intercambiar metadatos entre los hosts del clúster. Si algunos hosts del clúster de vSAN ejecutan versiones anteriores del software, se requiere una red de multidifusión. Para obtener más información sobre el uso de la multidifusión en un clúster de vSAN, consulte una versión anterior de *Administrar VMwarevSAN*.

NOTA: La siguiente configuración no es compatible: vCenter Server implementado en un clúster de vSAN 6.6 donde se utilizan direcciones IP de DHCP sin reservas. Es posible usar DHCP con reservas, ya que las direcciones IP asignadas se enlazan con las direcciones MAC de los puertos de VMkernel.

Asignar ancho de banda para vSAN mediante Network I/O Control

Si el tráfico de vSAN usa adaptadores de red físicos de 10 GbE que se comparten con otros tipos de tráfico del sistema, como tráfico de vSphere vMotion, tráfico de vSphere HA, tráfico de máquinas virtuales, etc., puede usar vSphere Network I/O Control en vSphere Distributed Switch para garantizar la cantidad de ancho de banda que se necesita para vSAN.

En vSphere Network I/O Control, puede configurar la reserva y los recursos compartidos para el tráfico saliente de vSAN.

- Configure una reserva para que Network I/O Control garantice que el ancho de banda mínimo esté disponible en el adaptador físico para vSAN.
- Configure recursos compartidos de modo que, cuando se sature el adaptador físico para vSAN, haya un cierto ancho de banda disponible para vSAN, y también para evitar que vSAN consuma toda la capacidad del adaptador físico durante las operaciones de recompilación y sincronización. Por ejemplo, es posible que el adaptador físico se sature cuando se produce un error en otro adaptador físico del equipo y todo el tráfico del grupo de puertos se transfiere a los demás adaptadores del equipo.

Por ejemplo, es posible configurar ciertos recursos compartidos y ancho de banda en un adaptador físico de 10 GbE que controla tráfico para vSAN, vSphere vMotion y máquinas virtuales.

Tabla 3-3. Ejemplo de configuración de Network I/O Control para un adaptador físico que controla vSAN

Tipo de tráfico	Reserva (Gbps)	Shares (Recursos compartidos)
vSAN	1	100
vSphere vMotion	0.5	70
Máquina virtual	0.5	30

Si el adaptador 10 GbE se satura, Network I/O Control asigna 5 Gbps a vSAN en el adaptador físico.

Para obtener más información sobre cómo utilizar vSphere Network I/O Control para configurar la asignación de ancho de banda para el tráfico de vSAN, consulte el documento *Redes de vSphere*.

Marcar el tráfico de vSAN

El etiquetado prioritario es un mecanismo que permite indicar a los dispositivos de red conectados que el tráfico de vSAN tiene grandes exigencias de calidad de servicio (Quality of Service, QoS). Puede asignar tráfico de vSAN a una determinada clase y, en consecuencia, marcar el tráfico con un valor de clase de servicio (Class of Service, CoS) de 0 (baja prioridad) a 7 (alta prioridad) mediante la directiva de filtrado y marcado de tráfico de vSphere Distributed Switch.

Segmentar el tráfico de vSAN en una VLAN

Considere la posibilidad de aislar el tráfico de vSAN en una VLAN a fin de obtener seguridad y rendimiento mejorados, especialmente si comparte la capacidad del adaptador físico de respaldo entre varios tipos de tráfico.

Tramas gigantes

Si tiene planificado usar tramas gigantes con vSAN para mejorar el rendimiento de las CPU, compruebe que las tramas gigantes estén habilitadas en todos los dispositivos de red y en todos los hosts del clúster.

De manera predeterminada, las características de descarga de segmentación TCP (TSO) y descarga de recepción grande (LRO) están habilitadas en ESXi. Evalúe si el uso de las tramas gigantes mejorará el rendimiento lo suficiente para justificar el costo que implica habilitarlas en todos los nodos de la red.

Crear rutas estáticas para redes de vSAN

Podría necesitar crear rutas estáticas en su entorno de vSAN.

En las configuraciones tradicionales en las que vSphere utiliza una puerta de enlace predeterminada única, todo el tráfico enrutado intenta llegar a su destino a través de esta puerta de enlace.

Sin embargo, determinadas implementaciones de vSAN podrían necesitar rutas estáticas. Por ejemplo, las implementaciones en las que el testigo está en otra red o la implementación de clúster ampliado en la que los sitios de datos y el host testigo están en sitios diferentes.

Para configurar rutas estáticas en sus hosts de ESXi, use el comando esxcli:

esxcli network ip route ipv4 add -n *remote-network* -g *gateway-to-use*

remote-network es la red remota a la que debe acceder su host y *gateway-to-use* es la interfaz que se debe utilizar cuando el tráfico se envía a la red remota.

Para obtener más información, consulte “Diseño de red para clústeres ampliados,” página 67.

Prácticas recomendadas para redes de vSAN

Tenga en cuenta las prácticas recomendadas de red de vSAN para mejorar el rendimiento y la capacidad de proceso.

- Para las configuraciones híbridas, dedique, al menos, un adaptador de red físico 1 GbE. Para obtener el mejor rendimiento de red, coloque el tráfico de vSAN en un adaptador físico 10 GbE dedicado o compartido.
- Para las configuraciones basadas íntegramente en tecnología flash, use un adaptador de red físico 10 GbE dedicado o compartido.
- Aprovisione una NIC física adicional como NIC de conmutación por error.
- Si usa un adaptador de red 10 GbE compartido, coloque el tráfico de vSAN en un conmutador distribuido y configure Network I/O Control para garantizar el ancho de banda de vSAN.

Diseñar y dimensionar dominios de errores de vSAN

La característica de dominios de errores de vSAN le ordena a vSAN que distribuya los componentes de redundancia entre los servidores de bastidores informáticos separados. De este modo, es posible proteger el entorno contra un error en el nivel de los bastidores como por ejemplo, una pérdida de la alimentación eléctrica o de la conectividad.

Construcciones de dominios de errores

vSAN requiere al menos dos dominios de errores, cada uno compuesto por uno o más hosts. Las definiciones de los dominios de errores deben reconocer las construcciones de hardware físico que pueden representar una zona de errores potencial como, por ejemplo, un gabinete individual de un bastidor informático.

De ser posible, use al menos cuatro dominios de errores. Tres dominios de errores no admiten determinados modos de evacuación de datos, y vSAN no puede volver a proteger los datos después de un error. En este caso, necesitará un dominio de errores adicional con capacidad para la reconstrucción, que no puede proporcionar con solo tres dominios de errores.

Si se habilitan los dominios de errores, vSAN aplica la directiva activa de almacenamiento de las máquinas virtuales a los dominios de errores y no solamente a los hosts individuales.

Calcule la cantidad de dominios de errores de un clúster en función del atributo **Primary level of failures to tolerate** (Nivel principal de errores que se toleran) o PFTT de las directivas de almacenamiento que planea asignar a las máquinas virtuales.

```
number of fault domains = 2 * PFTT + 1
```

Si un host no es miembro de un dominio de errores, vSAN lo interpreta como un dominio de errores independiente.

Usar dominios de errores para errores en varios hosts

Suponga que tiene un clúster que contiene cuatro bastidores de servidores, cada uno con dos hosts. Si **Nivel primario de errores que se toleran** se establece en uno y no se han habilitado los dominios de errores, es posible que vSAN almacene ambas réplicas de un objeto con hosts en el mismo gabinete de bastidor. De esta manera, es posible que las aplicaciones queden expuestas a una posible pérdida de datos ante un error en el nivel del bastidor. Cuando se configuran hosts que, potencialmente, pueden experimentar un error juntos en dominios de errores separados, vSAN garantiza que cada componente de protección (réplicas y testigos) se coloque en un dominio de errores diferente.

Si agrega hosts y capacidad, puede usar la configuración de dominios de errores actual o puede definir dominios de errores.

Para obtener una tolerancia a errores y una carga de almacenamiento equilibrada al utilizar dominios de errores, tenga en cuenta las siguientes directrices:

- Proporcione suficientes dominios de errores para satisfacer el atributo **Primary level of failures to tolerate** (Nivel principal de errores que se toleran) según se ha configurado en las directivas de almacenamiento.

  Defina, al menos, tres dominios de errores. Si desea obtener la mejor protección, defina un mínimo de cuatro dominios.

- Asigne la misma cantidad de hosts a cada dominio de errores.
- Use hosts con configuraciones uniformes.
- De ser posible, dedique un dominio de errores con capacidad libre para la reconstrucción de datos tras un error.

Usar dispositivos de arranque y vSAN

Iniciar la instalación de ESXi que forma parte de un clúster de vSAN desde un dispositivo flash supone ciertas restricciones.

Al arrancar un host de vSAN desde un dispositivo USB/SD, debe usar una unidad flash USB o SD de alta calidad de 4 GB o más.

Al arrancar un host de vSAN desde un dispositivo SATADOM, debe usar un dispositivo de celdas de un solo nivel (single-level cell, SLC). El tamaño del dispositivo de arranque debe ser de 16 GB como mínimo.

Durante la instalación, el instalador de ESXi crea una partición de volcado de núcleo en el dispositivo de arranque. El tamaño predeterminado de esta partición cumple con la mayoría de los requisitos de instalación.

Si la memoria del host ESXi es de 512 GB o menos, puede arrancar el host desde un dispositivo USB, SD o SATADOM. Si la memoria del host ESXi supera los 512 GB, debe arrancar el host desde un dispositivo de disco o SATADOM.

NOTA: vSAN 6.5 y versiones posteriores permiten cambiar el tamaño de una partición de volcado de núcleo existente en un host ESXi de un clúster de vSAN. Asimismo, permiten arrancar desde dispositivos USB/SD. Para obtener más información, consulte el artículo de la base de conocimientos de VMware en http://kb.vmware.com/kb/2147881.

Los hosts que arrancan desde un disco tienen un VMFS local. Si tiene un disco con un sistema VMFS que ejecuta máquinas virtuales, debe separar el disco para un arranque de ESXi que no se use para vSAN. En este caso, se precisan controladoras separadas.

Información de registro y dispositivos de arranque en vSAN

Cuando se arranca un host ESXi desde un dispositivo USB o SD, la información de registros y los rastros de la pila se pierden al reiniciarse el host. Esto se debe a que la partición temporal se encuentra en una unidad RAM. Use almacenamiento persistente para los registros, los rastros de la pila y los volcados de memoria.

No almacene información de registros en el almacén de datos de vSAN. Esta configuración no se admite porque un error en el clúster de vSAN podría afectar a la accesibilidad de la información de registros.

Tenga en cuenta las siguientes opciones para el almacenamiento persistente de registros:

- Use un dispositivo de almacenamiento que no se use para vSAN que tenga formato de VMFS o NFS.
- Configure ESXi Dump Collector y vSphere Syslog Collector en el host para enviar los volcados de memoria y los registros del sistema a vCenter Server.

Para obtener más información sobre la configuración de la partición temporal con una ubicación persistente, consulte el documento *Instalar y configurar vSphere*.

Registros persistentes en un clúster de vSAN

Proporcione almacenamiento para que se conserven los registros de los hosts en el clúster de vSAN.

Si instala ESXi en un dispositivo USB o SD, y asigna almacenamiento local a vSAN, es posible que no tenga espacio suficiente en el almacén de datos o en el almacenamiento local para los registros persistentes.

Para evitar una posible pérdida de información de registros, configure ESXi Dump Collector y vSphere Syslog Collector para que redirijan los registros del sistema y los volcados de memoria de ESXi a un servidor de red. Consulte la documentación de *Instalar y configurar vSphere*.

Preparar un clúster nuevo o existente para vSAN

4

Antes de habilitar vSAN en un clúster y comenzar a usarlo como almacenamiento de máquinas virtuales, proporcione la infraestructura necesaria para el funcionamiento correcto de vSAN.

Este capítulo cubre los siguientes temas:

Seleccionar o verificar la compatibilidad de los dispositivos de almacenamiento

Un paso importante antes de implementar vSAN es consultar la *Guía de compatibilidad de VMware* para comprobar que los dispositivos de almacenamiento, los controladores y el firmware sean compatibles con vSAN.

Existen varias opciones que puede seleccionar para la compatibilidad de vSAN.

- Use un servidor de vSAN Ready Node, un servidor físico que los proveedores OEM y VMware validan como compatible con vSAN.

- Ensamble un nodo seleccionando componentes individuales entre los modelos de dispositivos validados.

Sección de la *Guía de compatibilidad de VMware*	Tipo de componente para verificación
Sistemas	Servidor físico que ejecuta ESXi.
vSAN	■ Modelo de disco magnético SAS o SATA para configuraciones híbridas. ■ Modelo de dispositivo flash que se enumera en la *Guía de compatibilidad de VMware*. Ciertos modelos de dispositivos flash PCIe también pueden funcionar con vSAN. Tenga en cuenta, también, la resistencia de escritura y la clase de rendimiento. ■ Modelo de controladora de almacenamiento que admite acceso directo. vSAN puede funcionar con controladoras de almacenamiento configuradas para el modo de RAID 0 si cada dispositivo de almacenamiento se representa como un grupo RAID 0 individual.

Preparar el almacenamiento

Proporcione espacio de disco suficiente para vSAN y para las cargas de trabajo virtualizadas que usan el almacén de datos de vSAN.

Preparar los dispositivos de almacenamiento

Use discos magnéticos y dispositivos flash según los requisitos de vSAN.

Compruebe que el clúster disponga de la capacidad suficiente para admitir el consumo esperado de las máquinas virtuales y la configuración de **Primary level of failures to tolerate** (Nivel principal de errores que se toleran) en la directiva de almacenamiento para las máquinas virtuales.

Los dispositivos de almacenamiento deben cumplir con los siguientes requisitos para que vSAN pueda reclamarlos:

- Los dispositivos de almacenamiento son locales para los hosts ESXi. vSAN no puede reclamar dispositivos remotos.
- Los dispositivos de almacenamiento no tienen información sobre particiones existentes.
- En el mismo host, no es posible tener grupos de discos híbridos y también grupos de discos basados íntegramente en tecnología flash.

Preparar los dispositivos para los grupos de discos

Cada grupo de discos proporciona un dispositivo flash de almacenamiento en caché y, al menos, un disco magnético o un dispositivo de capacidad flash. La capacidad del dispositivo flash de almacenamiento en caché debe equivaler, al menos, al 10 % del almacenamiento que se espera que se consuma en el dispositivo de capacidad, sin las copias de protección.

vSAN requiere, como mínimo, un grupo de discos en un host que contribuya almacenamiento a un clúster compuesto por al menos tres hosts. Use hosts que tengan una configuración uniforme para obtener el mejor rendimiento de vSAN.

Capacidad útil y sin procesar

Proporcione una capacidad de almacenamiento sin procesar que sea superior a la capacidad de las máquinas virtuales para controlar determinados casos.

- No incluya el tamaño de los dispositivos flash de almacenamiento en caché como capacidad. Estos dispositivos no aportan almacenamiento y se utilizan como memoria caché, a menos que se hayan agregado dispositivos flash para almacenamiento.

- Proporcione suficiente espacio para controlar el valor de **Primary level of failures to tolerate** (Nivel principal de errores que se toleran) o PFTT en la directiva de almacenamiento de una máquina virtual. Un valor de PFTT superior a 0 extiende la superficie de memoria del dispositivo. Si el valor de PFTT se establece en 1, se duplica la superficie de memoria. Si el valor de PFTT se establece en 2, se triplica la superficie de memoria y así sucesivamente.
- Compruebe si el almacén de datos de vSAN cuenta con espacio suficiente para una operación. Para ello, examine el espacio en los hosts individuales en lugar del espacio en el objeto consolidado del almacén de datos de vSAN. Por ejemplo, al evacuar un host, es posible que todo el espacio libre del almacén de datos esté en el host que va a evacuar. El clúster no puede admitir la evacuación a otro host.
- Si las cargas de trabajo que tienen almacenamiento con aprovisionamiento fino comienzan a consumir una gran cantidad de almacenamiento, proporcione suficiente espacio para prevenir que se agote la capacidad del almacén de datos.
- Compruebe que el almacenamiento físico admita el modo de mantenimiento y reprotección de los hosts en el clúster de vSAN.
- Tenga en cuenta la sobrecarga de vSAN para el espacio de almacenamiento utilizable.
  - El formato en disco versión 1.0 agrega una sobrecarga adicional de aproximadamente 1 GB por dispositivo de capacidad.
  - El formato en disco versión 2.0 agrega una sobrecarga adicional, que generalmente no excede el 1-2 % de capacidad por dispositivo.
  - El formato en disco versión 3.0 y posteriores agrega una sobrecarga adicional, que generalmente no excede el 1-2 % de capacidad por dispositivo. La desduplicación y la compresión con la suma de comprobación de software habilitada requieren una sobrecarga adicional de aproximadamente 6,2 % de capacidad por dispositivo.

Para obtener más información sobre la planificación de la capacidad de los almacenes de datos de vSAN, consulte el documento *Guía de diseño y dimensionamiento de VMware vSAN*.

Impacto de la directiva de vSAN en la capacidad

La directiva de almacenamiento de vSAN para las máquinas virtuales afecta a los dispositivos de capacidad de diversas maneras.

Tabla 4-1. Directiva de máquina virtual de vSAN y capacidad en bruto

Aspectos de la incidencia de las directivas	Descripción
Cambios en las directivas	■ El valor de **Primary level of failures to tolerate** (Nivel principal de errores que se toleran) o PFTT incide en el espacio de almacenamiento físico que se debe suministrar para las máquinas virtuales. Cuando más alto es el valor de FTT para aumentar la disponibilidad, más espacio es necesario proporcionar. Cuando el valor de PFTT se establece en 1, se imponen dos réplicas del archivo VMDK para una máquina virtual. Con el valor de PFTT establecido en 1, un archivo VMDK de 50 GB requiere 100 GB de espacio en diferentes hosts. Si el valor de PFTT se cambia a 2, es necesario contar con espacio suficiente para admitir tres réplicas del archivo VMDK en los hosts del clúster (o 150 GB). ■ Algunos cambios de directivas, como un nuevo valor del atributo Number of disk stripes per object (Número de fracciones de disco por objeto), requieren recursos temporales. vSAN vuelve a crear los objetos afectados por el cambio. Durante un tiempo determinado, el almacenamiento físico debe alojar los objetos nuevos y antiguos.
Espacio disponible para el modo de mantenimiento o reprotección	Cuando coloca un host en modo de mantenimiento o clona una máquina virtual, puede que el almacén de datos no pueda evacuar los objetos de la máquina virtual, a pesar de que el almacén de datos de vSAN indique que hay suficiente espacio disponible. Esta falta de espacio puede producirse si el espacio libre se encuentra en el host que se va a colocar en modo de mantenimiento.

Marcar dispositivos flash como de capacidad mediante ESXCLI

Puede marcar manualmente los dispositivos flash de cada host como dispositivos de capacidad mediante esxcli.

Prerequisitos

Compruebe que esté usando vSAN 6.5 o una versión posterior.

Procedimiento

1 Para conocer el nombre del dispositivo flash que desea marcar como dispositivo de capacidad, ejecute el siguiente comando en cada host.

   a En ESXi Shell, ejecute el comando `esxcli storage core device list`.

   b Busque el nombre del dispositivo en la parte superior de la salida del comando y anótelo.

   El comando admite las siguientes opciones:

   Tabla 4-2. Opciones de comandos

Opciones	Descripción
`-d|--disk=str`	El nombre del dispositivo registro que desea etiquetar como dispositivo de capacidad. Por ejemplo, `mpx.vmhba1:C0:T4:L0`
`-t|--tag=str`	Especifique la etiqueta que desea agregar o quitar. Por ejemplo, la etiqueta `capacityFlash` se usa para marcar un dispositivo flash para capacidad.

   El comando muestra la información de todos los dispositivos identificados por ESXi.

2 En la salida, compruebe que el atributo `Is SSD` (Es SSD) para el dispositivo tenga el valor `true`.

3 Para etiquetar un dispositivo flash como de capacidad, ejecute el comando `esxcli vsan storage tag add -d <device name> -t capacityFlash`.

   Por ejemplo, el comando `esxcli vsan storage tag add -t capacityFlash -d mpx.vmhba1:C0:T4:L0`, donde `mpx.vmhba1:C0:T4:L0` es el nombre del dispositivo.

4 Compruebe si el dispositivo flash se ha marcado como de capacidad.

   a En la salida, identifique si el atributo `IsCapacityFlash` para el dispositivo tiene el valor `1`.

Ejemplo: Salida de comando

Puede ejecutar el comando `vdq -q -d <device name>` para comprobar el atributo `IsCapacityFlash`. Por ejemplo, la ejecución del comando `vdq -q -d mpx.vmhba1:C0:T4:L0` devuelve la siguiente salida.

```
\{
"Name"     : "mpx.vmhba1:C0:T4:L0",
"VSANUUID" : "",
"State"    : "Eligible for use by VSAN",
"ChecksumSupport": "0",
"Reason"   : "None",
"IsSSD"    : "1",
"IsCapacityFlash": "1",
"IsPDL"    : "0",
    \},
```

Desetiquetar dispositivos flash utilizados como dispositivos de capacidad mediante ESXCLI

Puede desetiquetar los dispositivos flash que se utilizan como dispositivos de capacidad, de modo que estén disponibles para almacenamiento en caché.

Procedimiento

1 Para desetiquetar un dispositivo flash como dispositivo de capacidad, ejecute el comando `esxcli vsan storage tag remove -d <device name> -t capacityFlash`. Por ejemplo, el comando `esxcli vsan storage tag remove -t capacityFlash -d mpx.vmhba1:C0:T4:L0`, donde `mpx.vmhba1:C0:T4:L0` es el nombre del dispositivo.

2 Compruebe si el dispositivo flash se desetiquetó.

   a En la salida, identifique si el atributo `IsCapacityFlash` para el dispositivo tiene el valor `0`.

Ejemplo: Salida de comando

Puede ejecutar el comando `vdq -q -d <device name>` para comprobar el atributo `IsCapacityFlash`. Por ejemplo, la ejecución del comando `vdq -q -d mpx.vmhba1:C0:T4:L0` devuelve la siguiente salida.

```
[
    \{
"Name"     : "mpx.vmhba1:C0:T4:L0",
"VSANUUID" : "",
"State"    : "Eligible for use by VSAN",
"ChecksumSupport": "0",
"Reason"   : "None",
"IsSSD"    : "1",
"IsCapacityFlash": "0",
"IsPDL"    : "0",
    \},
```

Marcar dispositivos flash como de capacidad mediante RVC

Ejecute el comando de RVC `vsan.host_claim_disks_differently` RVC para marcar dispositivos almacenamiento como dispositivos flash, dispositivos de capacidad o discos magnéticos (HDD).

Puede usar la herramienta RVC para etiquetar dispositivos flash como dispositivos de capacidad individualmente, o bien en lotes especificando el modelo del dispositivo. Al etiquetar dispositivos flash como dispositivos de capacidad, puede incluirlos en grupos de discos basados íntegramente en tecnología flash.

NOTA: El comando `vsan.host_claim_disks_differently` no comprueba el tipo de dispositivo antes de etiquetarlo. El comando etiqueta cualquier dispositivo que se anexe mediante la opción del comando `capacity_flash`, incluidos los discos magnéticos y los dispositivos que ya están en uso. Asegúrese de comprobar el estado del dispositivo antes de etiquetarlo.

Si desea obtener información sobre los comandos de RVC para la administración de vSAN, consulte la *Guía de referencia de los comandos de RVC*.

Prerequisitos

- Compruebe que esté usando vSAN 6.5 o una versión posterior.
- Compruebe que SSH esté habilitado en vCenter Server Appliance.

Procedimiento

1 Abra una conexión SSH a vCenter Server Appliance.

2 Inicie sesión en el dispositivo con una cuenta local que tenga privilegios de administrador.

3 Ejecute el comando siguiente para iniciar la herramienta RVC:

```
rvc local_user_name@target_vCenter_Server
```

Por ejemplo, si desea usar el mismo vCenter Server Appliance para marcar dispositivos flash para capacidad como usuario raíz, ejecute el comando siguiente:

```
rvc root@localhost
```

4 Escriba la contraseña para el usuario.

5 Desplácese hasta el directorio *`vcenter_server`*`/`*`data_center`*`/computers/`*`cluster`*`/hosts` en la infraestructura de vSphere.

6 Ejecute el comando `vsan.host_claim_disks_differently` con las opciones `--claim-type capacity_flash --model` *model_name* para marcar todos los dispositivos flash del mismo modelo como dispositivos de capacidad en todos los hosts del clúster.

```
vsan.host_claim_disks_differently --claim-type capacity_flash --model model_name *
```

Qué hacer a continuación

Habilite vSAN en el clúster y reclame dispositivos de capacidad.

Proporcionar memoria para vSAN

Debe aprovisionar hosts con memoria en función de la cantidad máxima de dispositivos y grupos de discos que desea asignar a vSAN.

Para satisfacer el caso de la cantidad máxima de dispositivos y grupos de discos, debe aprovisionar hosts con 32 GB de memoria para las operaciones del sistema. Para obtener información sobre la configuración máxima de dispositivos, consulte el documento *Valores máximos de configuración de vSphere*.

Preparar los hosts para vSAN

Como parte de la preparación para habilitar vSAN, consulte los requisitos y las recomendaciones sobre la configuración de hosts para el clúster.

- Compruebe que los dispositivos de almacenamiento incluidos en los hosts, al igual que las versiones de los controladores y el firmware correspondientes, aparezcan en la sección vSAN de la *Guía de compatibilidad de VMware*.
- Asegúrese de que al menos tres hosts aporten almacenamiento al almacén de datos de vSAN.
- Para las operaciones de mantenimiento y corrección de errores, agregue al menos cuatro hosts al clúster.
- Designe hosts que tengan una configuración uniforme para obtener el mejor equilibrio de almacenamiento en el clúster.
- No agregue al clúster los hosts que tengan solamente recursos informáticos para evitar una distribución desequilibrada de los componentes de almacenamiento de los hosts que aportan almacenamiento. Las máquinas virtuales que requieren mucho espacio de almacenamiento y que se ejecutan en hosts únicamente informáticos pueden almacenar una gran cantidad de componentes en hosts de capacidad individuales. Como consecuencia, es posible que disminuya el rendimiento de almacenamiento en el clúster.
- No configure directivas exigentes de administración de la energía de las CPU en los hosts para ahorrar energía. Ciertas aplicaciones que son sensibles a la latencia en la velocidad de las CPU pueden experimentar un rendimiento muy deficiente. Para obtener información sobre las directivas de administración de la energía de las CPU, consulte el documento *Administrar recursos de vSphere*.
- Si el clúster contiene servidores blade, considere la posibilidad de ampliar la capacidad del almacén de datos mediante un gabinete de almacenamiento externo que esté conectado a los servidores blade y que aparezca en la sección vSAN de la *Guía de compatibilidad de VMware*.
- Tenga en cuenta la configuración de las cargas de trabajo que coloque en una configuración híbrida o basada íntegramente en tecnología flash.
  - Para obtener niveles altos de rendimiento predecible, proporcione un clúster de grupos de discos basados íntegramente en tecnología flash.
  - Para obtener un equilibrio entre rendimiento y costo, proporcione un clúster de grupos de discos híbridos.

Compatibilidad de vSAN y vCenter Server

Sincronice las versiones de vCenter Server y ESXi a fin de evitar posibles errores debido a diferencias en la compatibilidad con vSAN en vCenter Server y ESXi.

Para obtener la mejor integración entre los componentes de vSAN en vCenter Server y ESXi, implemente la versión más reciente de los dos componentes de vSphere. Consulte los documentos *Instalar y configurar vSphere* y *Actualizar vSphere*.

Preparar controladoras de almacenamiento

Configure la controladora de almacenamiento en un host en función de los requisitos de vSAN.

Compruebe que las controladoras de almacenamiento en los hosts vSAN cumplan con ciertos requisitos para las características avanzadas y de modo, controladores, versión de firmware, profundidad de cola y almacenamiento en caché.

Tabla 4-3. Examinar la configuración de la controladora de almacenamiento para vSAN

Característica de la controladora de almacenamiento	Requisito de la controladora de almacenamiento
Modo requerido	■ Consulte en la *Guía de compatibilidad de VMware* los requisitos de vSAN para el modo requerido (de acceso directo o de RAID 0) de la controladora. ■ Si se admiten tanto el modo de acceso directo o como el de RAID 0, configure el modo de acceso directo y en lugar del modo de RAID0. RAID 0 implica complejidad para el reemplazo de discos.
Modo de RAID	■ En el caso de RAID 0, cree un volumen RAID para el dispositivo del disco físico. ■ Excepto el modo que se enumera en la *Guía de compatibilidad de VMware*, no habilite el modo de RAID. ■ No habilite la distribución de controladoras.
Versión de firmware y del controlador	■ Use la versión más reciente del firmware y del controlador para la controladora según la información proporcionada en la *Guía de compatibilidad de VMware*. ■ Si usa el controlador incluido en el paquete de la controladora, compruebe que esté certificado para vSAN. Es posible que las versiones de ESXi del fabricante del equipo original (OEM) contengan controladores que no estén certificados y que no figuren en la *Guía de compatibilidad de VMware*.
Profundidad de la cola	Compruebe que la profundidad de la cola de la controladora sea de 256 o superior. La profundidad de cola superior proporciona un rendimiento mejorado.
Memoria caché	Deshabilite la memoria caché de la controladora de almacenamiento o, en caso de que esto no sea posible, configúrela con un valor de lectura del 100 %.
Características avanzadas	Deshabilite las características avanzadas como HP SSD Smart Path.

Configurar la red de vSAN

Antes de habilitar vSAN en un clúster y en hosts ESXi, debe construir la red necesaria para transportar la comunicación de vSAN.

vSAN proporciona una solución de almacenamiento distribuida, que supone un intercambio de datos entre los hosts ESXi que participan en el clúster. La preparación de la red para la instalación de vSAN incluye ciertos aspectos de configuración.

Para obtener información sobre directrices para el diseño de redes, consulte "Diseñar la red de vSAN," página 31.

Poner hosts en la misma subred

Para obtener el mejor rendimiento de red, los hosts deben conectarse a la misma subred. En vSAN 6.0 y versiones posteriores, si es necesario, también se pueden conectar hosts en la misma red de capa 3.

Dedicar ancho de banda de red en un adaptador físico

Asigne un ancho de banda de al menos 1 Gbps para vSAN. Puede usar una de las siguientes opciones de configuración:

- Dedique adaptadores físicos 1 GbE para una configuración de host híbrida.
- Use adaptadores físicos 10 GbE dedicados o compartidos para las configuraciones basadas íntegramente en tecnología flash.

- De ser posible, use adaptadores físicos 10 GbE dedicados o compartidos para las configuraciones híbridas.
- Dirija el tráfico de vSAN en un adaptador físico 10 GbE que controle el tráfico del sistema y use vSphere Network I/O Control en un conmutador distribuido a fin de reservar ancho de banda para vSAN.

Configurar un grupo de puertos en un conmutador distribuido

Configure un grupo de puertos en un conmutador distribuido para vSAN.

- Asigne el adaptador físico de vSAN al grupo de puertos como un vínculo superior activo.

  En el caso de un equipo de tarjetas NIC para disponibilidad de red, seleccione un algoritmo de formación de equipos en función de la conexión de los adaptadores físicos al conmutador.
- Si se ha diseñado, asigne el tráfico de vSAN a una VLAN habilitando el etiquetado en el conmutador virtual.

Examinar el firewall en un host para vSAN

vSAN envía mensajes en ciertos puertos en cada host del clúster. Compruebe que los firewalls del host permitan el tráfico en estos puertos.

Tabla 4-4. Puertos en los hosts en vSAN

Servicio de vSAN	Dirección del tráfico	Nodos de comunicación	Protocolo de transporte	Puerto
Proveedor de vSAN (vsanvp)	Entrante y saliente	vCenter Server y ESXi	TCP	8080
Servicio de clústeres de vSAN		ESXi	UDP	12345, 23451
Transporte de vSAN		ESXi	TCP	2233
Agente de unidifusión		ESXi	UDP	12321

Consideraciones acerca de la licencia de vSAN

Cuando prepare el clúster para vSAN, consulte los requisitos de la licencia de vSAN.

- Asegúrese de haber obtenido una licencia válida para control completo de configuración del host en el clúster. La licencia debe ser distinta a la que utilizó para fines de evaluación.

  Después de que caduque la licencia o el período de evaluación de vSAN, podrá seguir usando la configuración actual de los recursos de vSAN. Sin embargo, no podrá agregar capacidad a un grupo de discos ni tampoco crear grupos de discos.
- Si el clúster está compuesto por grupos de discos basados íntegramente en tecnología flash, asegúrese de que la característica de componentes basados íntegramente en tecnología flash esté disponible con su licencia.
- Si el clúster de vSAN utiliza características avanzadas como la desduplicación y la compresión o el clúster ampliado, verifique que dicha característica esté disponible con su licencia.

- Tenga en cuenta la capacidad de CPU de la licencia vSAN en el clúster al agregar o quitar hosts en el clúster.

  Las licencias de vSAN ofrecen capacidad por CPU. Cuando asigne una licencia de vSAN a un clúster, la cantidad de capacidad de licencia que se utiliza es igual a la cantidad total de CPU de los hosts que participan en el clúster.

Crear un clúster de vSAN 5

Puede activar vSAN al crear un clúster o habilitar vSAN en los clústeres existentes.

Este capítulo cubre los siguientes temas:

Características de un clúster de vSAN

Antes de trabajar en un entorno de vSAN, debe conocer las características de un clúster de vSAN.

Un clúster de vSAN incluye las siguientes características:

- Es posible tener varios clústeres de vSAN para cada instancia de vCenter Server. Es posible usar un solo vCenter Server para administrar más de un clúster de vSAN.
- vSAN utiliza capacidad de todos los dispositivos, incluidos los dispositivos flash de memoria caché y de capacidad, y no comparte dispositivos con otras funciones.
- Los clústeres de vSAN pueden incluir hosts con o sin dispositivos de capacidad. El requisito mínimo es de tres hosts con dispositivos de capacidad. Para obtener mejores resultados, cree un clúster de vSAN con hosts configurados de manera uniforme.
- Si un aporta capacidad, debe tener, al menos, un dispositivo flash de almacenamiento en caché y un dispositivo de capacidad.
- En los clústeres híbridos, se utilizan discos magnéticos para los dispositivos flash y de capacidad para la memoria caché de lectura y de escritura. vSAN asigna el 70 % de la memoria caché disponible para lectura y el 30 % restante para el búfer de escritura. En estas configuraciones, los dispositivos flash funcionan como una memoria caché de lectura y un búfer de escritura.
- En un clúster basado íntegramente en tecnología flash, hay un dispositivo flash designado que se utiliza como memoria caché de lectura y dispositivos flash adicionales que se utilizan para capacidad. En los clústeres basados íntegramente en tecnología flash, todas las solicitudes provienen directamente de la capacidad del grupo flash.
- Solamente los dispositivos de capacidad locales o con conexión directa pueden participar en un clúster de vSAN. vSAN no puede utilizar capacidad de otros sistemas de almacenamiento externos, como SAN o NAS, conectados al clúster.

Para conocer las prácticas recomendadas sobre el diseño y el dimensionamiento de un clúster de vSAN, consulte Capítulo 3, "Diseñar y dimensionar un clúster de vSAN," página 21.

Antes de crear un clúster de vSAN

Este tema proporciona una lista de verificación de los requisitos de software y hardware para la creación de un clúster de vSAN. También puede usar la lista de verificación para comprobar que el clúster cumpla con las directrices y con los requisitos básicos.

Requisitos de clúster de vSAN

Antes de comenzar, consulte los modelos específicos de los dispositivos de hardware, así como las versiones específicas de los controladores y del firmware, en el sitio web de la Guía de compatibilidad de VMware, en la siguiente URL: http://www.vmware.com/resources/compatibility/search.php. La siguiente tabla muestra los requisitos clave de software y hardware que admite vSAN.

ADVERTENCIA: El uso de componentes de software y hardware, controladores, controladoras y firmware no certificados puede provocar pérdida de datos y problemas de rendimiento inesperados.

Tabla 5-1. Requisitos de clúster de vSAN

Requisitos	Descripción
Hosts ESXi	■ Compruebe que esté usando la versión más reciente de ESXi en los hosts. ■ Compruebe que haya al menos tres hosts ESXi con configuraciones de almacenamiento compatibles disponibles para asignar al clúster de vSAN. Para obtener mejores resultados, configure el clúster de vSAN con cuatro hosts o más.
Memoria	■ Compruebe que cada host tenga un mínimo de 8 GB de memoria. ■ Para las configuraciones más grandes y para obtener un mejor rendimiento, se debe tener un mínimo de 32 GB de memoria en el clúster. Consulte "Diseñar y dimensionar hosts de vSAN," página 29.
Controladores, firmware y controladoras de E/S	■ Compruebe que las versiones de los controladores, del firmware y de las controladoras de E/S de almacenamiento estén certificadas y se enumeren en el sitio web de VCG, en la siguiente URL: http://www.vmware.com/resources/compatibility/search.php. ■ Compruebe que la controladora esté configurada para el modo de acceso directo o de RAID 0. ■ Compruebe que las características avanzadas y la memoria caché de la controladora estén deshabilitadas. Si no puede deshabilitar la memoria caché, debe configurar la memoria caché de lectura en el 100 %. ■ Compruebe que esté usando las controladoras con la profundidad de cola más alta. El uso de controladoras con una profundidad de cola inferior a 256 puede afectar de manera considerable el rendimiento de las máquinas virtuales durante el mantenimiento y los errores.
Memoria caché y de capacidad	■ Compruebe que los hosts vSAN que aportan almacenamiento al clúster tengan, al menos, un dispositivo de memoria caché y un dispositivo de capacidad. vSAN requiere acceso exclusivo a los dispositivos de capacidad y de memoria caché local de los hosts del clúster de vSAN. No puede compartir estos dispositivos con otros usos, como el sistema de archivos Virtual Flash File System (VFFS), las particiones de VMFS o una partición de arranque de ESXi. ■ Para obtener mejores resultados, cree un clúster de vSAN con hosts configurados de manera uniforme.

Tabla 5-1. Requisitos de clúster de vSAN (Continua)

Requisitos	Descripción
Conectividad de red	■ Compruebe que cada host esté configurado con, al menos, un adaptador de red. ■ Para las configuraciones híbridas, compruebe que los hosts de vSAN tengan un ancho de banda dedicado mínimo de 1 GbE. ■ Para las configuraciones basadas íntegramente en tecnología flash, compruebe que los hosts de vSAN tengan un ancho de banda mínimo de 10 GbE. Para obtener información de prácticas recomendadas y consideraciones sobre el diseño de la red de vSAN, consulte "Diseñar la red de vSAN," página 31 y "Requisitos de red para vSAN," página 19.
Compatibilidad de vSAN y vCenter Server	Compruebe que esté usando la versión más reciente de vCenter Server.
Clave de licencia	■ Compruebe que tenga una clave de licencia válida para vSAN. ■ Para utilizar la función basada íntegramente en tecnología flash, la licencia debe admitir esta capacidad. ■ Para utilizar las funciones avanzadas, como los clústeres ampliados o la desduplicación y la compresión, la licencia debe admitir esas funciones. ■ Compruebe que la cantidad de capacidad de licencia que planea utilizar sea igual a la cantidad total de CPU en los hosts que participan en el clúster de vSAN. No proporcione capacidad de licencia únicamente a los hosts que proporcionen capacidad al clúster. Si desea obtener información sobre las licencias para vSAN, consulte *Administrar vCenter Server y hosts*.

Para obtener información detallada sobre los requisitos de los clústeres de vSAN, consulte Capítulo 2, "Requisitos para habilitar vSAN," página 17.

Para obtener información exhaustiva sobre el diseño y el dimensionamiento de un clúster de vSAN, consulte la *guía de diseño y dimensionamiento de VMware vSAN*.

Habilitar vSAN

Para utilizar vSAN, debe crear un clúster de hosts y habilitar vSAN en el clúster.

Un clúster de vSAN puede incluir hosts con y sin capacidad. Al crear un clúster de vSAN, siga estas directrices.

- Un clúster de vSAN debe incluir un mínimo de tres hosts ESXi. Para que un clúster de vSAN tolere los errores de los hosts y los dispositivos, al menos tres hosts que se unan al clúster de vSAN deben aportar capacidad al clúster. Para obtener mejores resultados, considere la posibilidad de agregar cuatro hosts o más que aporten capacidad al clúster.
- Solo los hosts ESXi 5.5 Update 1 o posteriores pueden unirse al clúster de vSAN.
- Todos los hosts del clúster de vSAN deben tener el mismo formato en disco.
- Antes de transferir un host de un clúster de vSAN a otro clúster, asegúrese de que el clúster de destino sea compatible con vSAN.
- Para poder acceder al almacén de datos de vSAN, un host ESXi debe ser miembro del clúster de vSAN.

Después de habilitar vSAN, el proveedor de almacenamiento de vSAN se registra automáticamente con vCenter Server y se crea el almacén de datos de vSAN. Para obtener información sobre proveedores de almacenamiento, consulte el documento *Almacenamiento de vSphere*.

Configurar una red de VMkernel para vSAN

Para habilitar el intercambio de datos en el clúster de vSAN, debe proporcionar un adaptador de red de VMkernel para el tráfico de vSAN en cada host ESXi.

Procedimiento

1. En vSphere Web Client, desplácese hasta el host.
2. Haga clic en la pestaña **Configurar**.
3. En **Networking** (Redes), seleccione **VMkernel adapters** (Adaptadores de VMkernel).
4. Haga clic en el icono **Add host networking** (Agregar redes de host) ( ) para abrir el asistente Add Networking (Agregar redes).
5. En la página Select connection type (Seleccionar tipo de conexión), seleccione **VMkernel Network Adapter** (Adaptador de red de VMkernel) y haga clic en **Next** (Siguiente).
6. Configure el dispositivo de conmutación de destino.
7. En la página Port properties (Propiedades de puerto), seleccione **vSAN traffic** (Tráfico de vSAN).
8. Complete la configuración del adaptador de VMkernel.
9. En la página Listo para completar, verifique que vSAN esté habilitado en el estado del adaptador de VMkernel y haga clic en **Finalizar**.

La red de vSAN está habilitada para el host.

Qué hacer a continuación

Puede habilitar vSAN en el clúster del host.

Crear un clúster de vSAN

Al crear un clúster, puede habilitar vSAN.

Procedimiento

1. Haga clic con el botón derecho en un centro de datos de vSphere Web Client y seleccione **New Cluster** (Clúster nuevo).
2. Escriba un nombre para el clúster en el cuadro de texto **Name** (Nombre).

   Este nombre aparece en el navegador de vSphere Web Client.
3. Active la casilla **Turn ON** (Activar) de vSAN y haga clic en **OK** (Aceptar).

   El clúster aparecerá en el inventario.
4. Agregue hosts al clúster de vSAN. Consulte "Agregar un host al clúster de vSAN," página 120.

   Los clústeres de vSAN pueden incluir hosts con o sin dispositivos de capacidad. Para obtener los mejores resultados, agregue hosts con capacidad.

Al habilitar vSAN, se crea un almacén de datos de vSAN y se registra el proveedor de almacenamiento de vSAN. Los proveedores de almacenamiento de vSAN son componentes de software integrados que comunican las funcionalidades de almacenamiento del almacén de datos a vCenter Server.

Qué hacer a continuación

Compruebe que se haya creado el almacén de datos de vSAN. Consulte "Ver el almacén de datos de vSAN," página 55.

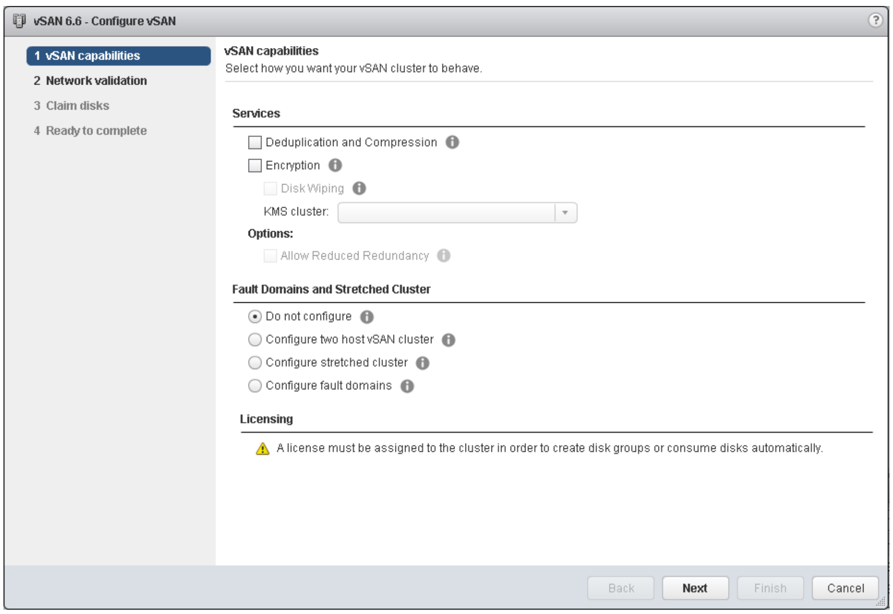
Compruebe que el proveedor de almacenamiento de vSAN esté registrado. Consulte "Ver los proveedores de almacenamiento de vSAN," página 139.

Puede reclamar los dispositivos de almacenamiento o crear grupos de discos. Consulte Capítulo 10, "Administrar dispositivos en un clúster de vSAN," página 109.

Configure el clúster de vSAN. Consulte "Configurar un clúster para vSAN," página 51.

Configurar un clúster para vSAN

Puede utilizar el asistente Configurar vSAN para completar la configuración básica del clúster de vSAN.



Prerequisitos

Debe configurar un clúster y agregar hosts al clúster antes de utilizar el asistente Configurar vSAN para completar la configuración básica.

Procedimiento

1 Desplácese hasta un clúster existente en vSphere Web Client.

2 Haga clic en la pestaña **Configurar**.

3 En vSAN, seleccione **General** y haga clic en el botón **Configure** (Configurar).

4 Seleccione **vSAN capabilities** (Funcionalidades de vSAN).

   a (Opcional) Active la casilla **Deduplication and Compression** (Desduplicación y compresión) si desea habilitar la desduplicación y compresión en el clúster.

   Puede activar la casilla **Permitir redundancia reducida** para habilitar la desduplicación y la compresión en un clúster de vSAN con recursos limitados, como un clúster de tres hosts en la que la opción **Nivel primario de errores que se toleran** se establece en 1. Si permite la redundancia reducida, es posible que los datos estén en riesgo durante la operación de reformateo de disco.

   b (Opcional) Active la casilla **Encryption** (Cifrado) si desea habilitar el cifrado de datos en reposo y seleccione un KMS.

c Seleccione el modo de tolerancia ante errores del clúster.

Opción	Descripción
Do not configure (No configurar)	Configuración predeterminada utilizada para un clúster de vSAN de un solo sitio.
Configurar el clúster de vSAN con dos hosts	Proporciona tolerancia ante errores para un clúster que tiene dos hosts en la oficina remota, con un host testigo en la oficina principal. Establezca la directiva **Primary level of failures to tolerate** (Nivel principal de errores que se toleran) en 1.
Configurar el clúster ampliado	Admite dos sitios activos, incluso con un número par de hosts y dispositivos de almacenamiento, y un host testigo en el tercer sitio.
Configure fault domains (Configurar dominios de errores)	Admite dominios de errores que puede utilizar para agrupar hosts de vSAN que podrían fallar en conjunto. Asigne uno o más hosts a cada dominio de errores.

d Puede activar la casilla **Permitir redundancia reducida** para habilitar el cifrado o la desduplicación y la compresión en un clúster de vSAN con recursos limitados. Por ejemplo, cuando el clúster tiene tres hosts con la opción **Primary level of failures to tolerate** (Nivel principal de errores que se toleran) establecida en 1. Si permite la redundancia reducida, es posible que los datos estén en riesgo durante la operación de reformateo de disco.

5 Haga clic en **Next** (Siguiente).

6 En la página Validación de red compruebe la configuración para los adaptadores de VMkernel de vSAN y haga clic en **Siguiente**.

7 En la página Claim disks (Reclamar discos), seleccione los discos que utilizará el clúster y haga clic en **Next** (Siguiente).

En cada host que aporte almacenamiento, seleccione un dispositivo flash para el nivel de memoria caché y uno o más dispositivos para el nivel de capacidad.

8 Siga el asistente para completar la configuración del clúster, según el modo de tolerancia ante errores.

a Si seleccionó **Configure two host vSAN cluster** (Configurar clúster de vSAN de dos hosts), seleccione un host testigo para el clúster y reclame los discos para el host testigo.

b Si seleccionó **Configure stretched cluster** (Configurar clúster ampliado), defina los dominios de errores para el clúster, seleccione un host testigo y recupere los discos para el host testigo.

c Si seleccionó **Configure fault domains** (Configurar dominios de errores), defina los dominios de errores para el clúster.

Para obtener más información sobre los dominios de errores, consulte "Administrar dominios de errores en clústeres de vSAN," página 126.

Para obtener más información sobre los clústeres ampliados, consulte Capítulo 6, "Extender un almacén de datos a dos sitios con clústeres ampliados," página 63.

9 En la página Ready to complete (Listo para finalizar), revise la configuración y haga clic en **Finish** (Finalizar).

Editar la configuración de vSAN

Puede editar la configuración del clúster de vSAN para cambiar el método para reclamar discos y para habilitar la desduplicación y la compresión.

Edite la configuración de un clúster de vSAN existente si desea habilitar la desduplicación y la compresión, o para cambiar el método de cifrado. Si habilita la desduplicación y la compresión, o el cifrado, el formato en disco del clúster se actualiza automáticamente a la versión más reciente.

Procedimiento

1 Desplácese hasta el clúster del host de vSAN en vSphere Web Client.

2 Haga clic en la pestaña **Configurar**.

3 En vSAN, seleccione **General**.

4 En el panel vSAN está activado, haga clic en el botón **Editar**.

5 (Opcional) Si desea habilitar la desduplicación y compresión en el clúster, marque la casilla Deduplication and compression (Desduplicación y compresión).

   vSAN actualizará automáticamente el formato en disco, lo que provocará un reformateo sucesivo de cada grupo de discos del clúster.

6 (Opcional) Si desea habilitar el cifrado en el clúster, marque la casilla Encryption (Cifrado) y seleccione un servidor KMS.

   vSAN actualizará automáticamente el formato en disco, lo que provocará un reformateo sucesivo de cada grupo de discos del clúster.

7 Haga clic en **OK** (Aceptar).

Habilitar vSAN en un clúster existente

Puede editar las propiedades de un clúster a fin de habilitar vSAN para un clúster existente.

Después de habilitar vSAN en el clúster, no podrá mover hosts de vSAN desde un clúster habilitado para vSAN a un clúster que no sea de vSAN.

Prerequisitos

Compruebe que el entorno cumpla con todos los requisitos. Consulte Capítulo 2, “Requisitos para habilitar vSAN,” página 17.

Procedimiento

1 Desplácese hasta un clúster del host existente en vSphere Web Client.

2 Haga clic en la pestaña **Configurar**.

3 En vSAN, seleccione **General** y haga clic en **Edit** (Editar) para editar la configuración del clúster.

4 Si desea habilitar la desduplicación y la compresión en el clúster, active la casilla Deduplication and compression (Desduplicación y compresión).

   vSAN actualiza automáticamente el formato en disco, lo que provoca que se vuelva a formatear de forma gradual cada grupo de discos en el clúster.

5 (Opcional) Si desea habilitar el cifrado en el clúster, marque la casilla Encryption (Cifrado) y seleccione un servidor KMS.

   vSAN actualiza automáticamente el formato en disco, lo que provoca que se vuelva a formatear de forma gradual cada grupo de discos en el clúster.

6 Haga clic en **OK** (Aceptar).

Qué hacer a continuación

Puede reclamar los dispositivos de almacenamiento o crear grupos de discos. Consulte Capítulo 10, “Administrar dispositivos en un clúster de vSAN,” página 109.

Deshabilitar vSAN

Puede desactivar vSAN para un clúster de host.

Cuando se deshabilita el clúster de vSAN, todas las máquinas virtuales ubicadas en el almacén de datos compartido de vSAN dejan de estar accesibles. Si va a usar la máquina virtual mientras vSAN está deshabilitado, asegúrese de migrar las máquinas virtuales del almacén de datos de vSAN a otro almacén de datos antes de deshabilitar el clúster de vSAN.

Prerequisitos

Compruebe que los hosts estén en modo de mantenimiento.

Procedimiento

1 Desplácese hasta el clúster del host en vSphere Web Client.

2 Haga clic en la pestaña **Configurar**.

3 En vSAN, seleccione **General** y haga clic en **Editar** para editar la configuración de vSAN.

4 Desactive la casilla **Turn On** (Activar) de vSAN.

Configurar los ajustes de licencia para un clúster de vSAN

Debe asignar una licencia a un clúster de vSAN antes de que venzan el período de evaluación o la licencia asignada actualmente.

Si actualiza, combina o divide licencias de vSAN, deberá asignar las licencias nuevas a clústeres de vSAN. Cuando asigna una licencia de vSAN a un clúster, la cantidad de capacidad de licencia que se utiliza es igual a la cantidad total de CPU de los hosts que participan en el clúster. La utilización de licencias del clúster de vSAN se recalcula y se actualiza cada vez que agrega o elimina un host del clúster. Para desea obtener sobre la administración de licencias y sobre la terminología y las definiciones de licencias, consulte el documento sobre la *administración de vCenter Server y hosts*.

Si se habilita vSAN en un clúster, se puede utilizar vSAN en el modo de evaluación para explorar sus características. El período de evaluación se inicia cuando se habilita vSAN y caduca después de 60 días. Para utilizar vSAN, debe otorgar una licencia al clúster antes de que venza el período de evaluación. Al igual que las licencias de vSphere, las licencias de vSAN tienen una capacidad por CPU. Algunas características avanzadas, como la configuración basada íntegramente en tecnología flash y los clústeres ampliados, requieren una licencia que admita la característica.

Prerequisitos

- Para ver y administrar las licencias de vSAN, debe tener el privilegio de **licencias .globales** en los sistemas vCenter Server, donde se ejecuta vSphere Web Client.

Procedimiento

1 En vSphere Web Client, desplácese hasta el clúster en el que ha habilitado vSAN.

2 Haga clic en la pestaña **Configurar**.

3 En **Configuration** (Configuración), seleccione **Licensing** (Concesión de licencias) y haga clic en **Assign License** (Asignar licencia).

4 Seleccione una opción de concesión de licencias.

   - Seleccione una licencia existente y haga clic en **OK** (Aceptar).
   - Cree una licencia de vSAN.

     a Haga clic en el icono **Create New License** (Crear nueva licencia)([Crear licencia]).

b En el cuadro de diálogo Licencias nuevas, introduzca o copie y pegue una clave de licencia de vSAN y haga clic en **Siguiente**.

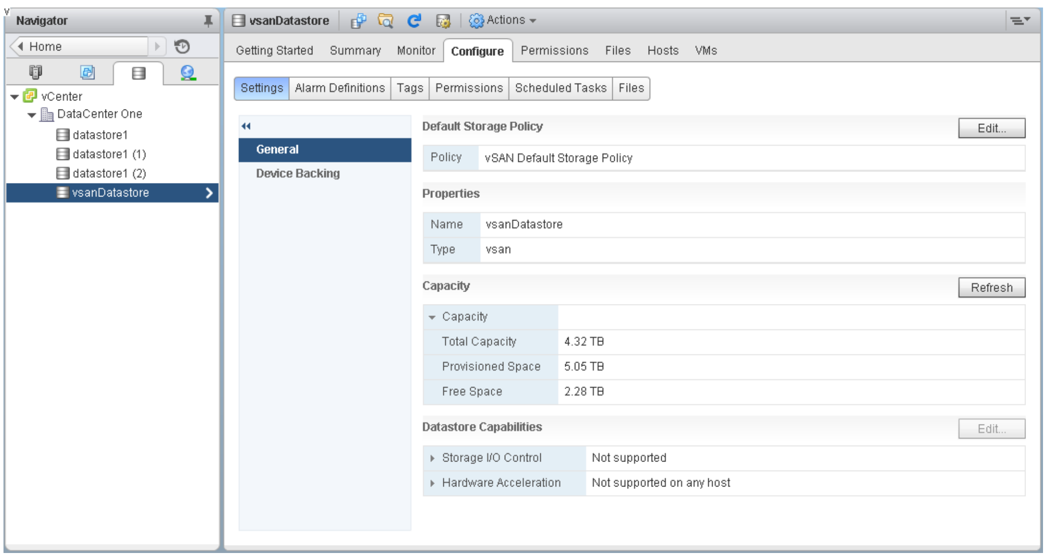
c En la página Edit license names (Editar nombres de licencias), cambie el nombre de la licencia nueva según corresponda y haga clic en **Next** (Siguiente).

d Haga clic en **Finish** (Finalizar).

e En el cuadro de diálogo Asignar licencia, seleccione la nueva licencia creada y haga clic en **Aceptar**.

Ver el almacén de datos de vSAN

Después de activar vSAN, se crea un solo almacén de datos. Puede revisar la capacidad del almacén de datos de vSAN.



Prerequisitos

Active vSAN y configure los grupos de discos.

Procedimiento

1 Desplácese hasta Storage (Almacenamiento) en vSphere Web Client.

2 Seleccione el almacén de datos de vSAN.

3 Haga clic en la pestaña **Configurar**.

4 Revise la capacidad del almacén de datos de vSAN.

El tamaño del almacén de datos de vSAN depende de la cantidad de dispositivos de capacidad por cada host ESXi de la cantidad de hosts ESXi en el clúster. Por ejemplo, si un host tiene siete dispositivos de capacidad de 2 TB y el clúster incluye ocho hosts, la capacidad de almacenamiento aproximada sería: 7 x 2 TB x 8 = 112 TB. Tenga en cuenta que al usar una configuración basada íntegramente en tecnología flash, se utilizan dispositivos flash para la capacidad. Para las configuraciones híbridas, se utilizan discos magnéticos para la capacidad.

Algo de capacidad se asigna para los metadatos.

- El formato en disco versión 1.0 agrega aproximadamente 1 GB por dispositivo de capacidad.
- El formato en disco versión 2.0 agrega una sobrecarga de capacidad, que generalmente no excede el 1-2 % de capacidad por dispositivo.

- El formato en disco versión 3.0 y posteriores agrega una sobrecarga de capacidad, que generalmente no excede el 1-2 % de capacidad por dispositivo. La desduplicación y la compresión con la suma de comprobación de software habilitada requieren una sobrecarga adicional de aproximadamente 6,2 % de capacidad por dispositivo.

Qué hacer a continuación

Use las funcionalidades de almacenamiento del almacén de datos de vSAN para crear una directiva de almacenamiento para las máquinas virtuales. Para obtener información, consulte el documento *Almacenamiento de vSphere*.

Usar vSAN y vSphere HA

Puede habilitar vSphere HA y vSAN en el mismo clúster. Al igual que con los almacenes de datos tradicionales, vSphere HA proporciona el mismo nivel de protección para las máquinas virtuales en los almacenes de datos de vSAN. El nivel de protección impone restricciones específicas cuando interactúan vSphere HA y vSAN.

Requisitos del host ESXi

Puede usar vSAN con un clúster de vSphere HA solamente si se satisfacen las siguientes condiciones:

- Todos los hosts ESXi del clúster deben corresponder a la versión 5.5 Update 1 o posterior.
- El clúster debe tener un mínimo de tres hosts ESXi. Para obtener mejores resultados, configure el clúster de vSAN con cuatro hosts o más.

Diferencias de red

vSAN usa su propia red lógica. Cuando vSAN y vSphere HA están habilitados para el mismo clúster, el tráfico entre agentes de HA se envía por medio de la red de almacenamiento y no por medio de la red de administración. vSphere HA usa la red de administración solamente cuando vSAN está deshabilitado. vCenter Server elige la red apropiada cuando vSphere HA está configurado en un host.

NOTA: Debe deshabilitar vSphere HA antes de habilitar vSAN en el clúster. A continuación, puede volver a habilitar vSphere HA.

Cuando solo se puede acceder parcialmente a una máquina virtual en todas las particiones de red, no es posible encender la máquina virtual ni obtener acceso completo a ella en ninguna partición. Por ejemplo, si un clúster se particiona en P1 y P2, el objeto del espacio de nombres de la máquina virtual está accesible para la partición P1 y no para P2. El VMDK está accesible para la partición P2 y no para P1. En estos casos, no es posible encender la máquina virtual ni obtener acceso completo a ella en ninguna partición.

En la siguiente tabla, se muestran las diferencias de red de vSphere HA, según si se usa o no vSAN.

Tabla 5-2. Diferencias de red de vSphere HA

	vSAN habilitado	vSAN deshabilitado
Red utilizada por vSphere HA	Red de almacenamiento de vSAN	Red de administración
Almacenes de datos de latidos	Cualquier almacén de datos montado en más de un host, pero no almacenes de datos de vSAN	Cualquier almacén de datos montado en más de un host
Host declarado aislado	Direcciones de aislamiento a las que no se puede hacer ping y red de almacenamiento de vSAN inaccesible	No se puede hacer ping a las direcciones de aislamiento y la red de administración no está accesible

Si cambia la configuración de red de vSAN, los agentes de vSphere HA no adquieren los nuevos parámetros de red de manera automática. Para realizar cambios en la red de vSAN, debe volver a habilitar la supervisión de hosts para el clúster de vSphere HA mediante vSphere Web Client:

1 Deshabilite la supervisión de hosts para el clúster de vSphere HA.
2 Efectúe los cambios en la red de vSAN.
3 Haga clic con el botón derecho en todos los hosts y seleccione **Reconfigure HA** (Volver a configurar HA).
4 Vuelva a habilitar la supervisión de hosts para el clúster de vSphere HA.

Configurar reserva de capacidad

Cuando se reserva capacidad para el clúster de vSphere HA con una directiva de control de admisión, este parámetro de configuración debe estar coordinado con la configuración correspondiente de la directiva **Nivel primario de errores que se toleran** en el conjunto de reglas de vSAN y no debe ser inferior a la capacidad reservada por el parámetro de configuración de control de admisión de vSphere HA. Por ejemplo, si el conjunto de reglas de vSAN solamente permite dos errores, la directiva de control de admisión de vSphere HA debe reservar una capacidad que sea equivalente a los errores de solamente un host o dos hosts. Si usa la directiva Percentage of Cluster Resources Reserved (Porcentaje de recursos del clúster reservados) para un clúster que tiene ocho hosts, no debe reservar más del 25 % de los recursos del clúster. En el mismo clúster, con la directiva **Primary level of failures to tolerate** (Nivel principal de errores que se toleran), la configuración no debe ser superior a dos hosts. Si vSphere HA reserva menos capacidad, la actividad de conmutación por error puede ser impredecible. La reserva de capacidad en exceso restringe el encendido de las máquinas virtuales y las migraciones entre clústeres de vSphere vMotion. Para obtener información sobre la directiva Percentage of Cluster Resources Reserved (Porcentaje de recursos del clúster reservados), consulte el documento *Disponibilidad de vSphere*.

Comportamiento de vSAN y vSphere HA ante un error en varios hosts

Después de que se produzca un error en un clúster de vSAN con una pérdida de quórum de conmutación por error para un objeto de una máquina virtual, es posible que vSphere HA no pueda reiniciar la máquina virtual aunque se restaure el quórum de clúster. vSphere HA garantiza el reinicio únicamente cuando tiene quórum de clúster y puede acceder a la copia más reciente del objeto de la máquina virtual. La copia más reciente es la última copia que se escribió.

Piense en un ejemplo en el que se aprovisiona una máquina virtual de vSAN para tolerar un error de host. La máquina virtual se ejecuta en un clúster de vSAN que incluye tres hosts: H1, H2 y H3. Se produce un error de manera secuencial en los tres hosts, donde H3 es el último en experimentar el error.

Una vez que H1 y H2 se recuperan, el clúster tiene quórum (se tolera un error de host). A pesar de este quórum, vSphere HA no puede reiniciar la máquina virtual porque el último host que experimentó el error (H3) contiene la copia más reciente del objeto de la máquina virtual y aún está inaccesible.

En este ejemplo, los tres hosts deben recuperarse al mismo tiempo o el quórum de dos hosts debe incluir el host H3. Si no se cumple ninguna de estas condiciones, HA intenta reiniciar la máquina virtual cuando el host H3 vuelve a estar en línea.

Implementar vSAN con vCenter Server Appliance

Es posible crear un clúster de vSAN a medida que se implementa una instancia de vCenter Server Appliance, y alojar el dispositivo en ese clúster.

vCenter Server Appliance es una máquina virtual Linux preconfigurada, que se utiliza para ejecutar VMware vCenter Server en sistemas Linux. Esta función permite configurar un clúster de vSAN en hosts ESXi nuevos sin utilizar vCenter Server.

Cuando se utiliza el instalador de vCenter Server Appliance para implementar una instancia de vCenter Server Appliance, es posible crear un clúster de vSAN de host único, y la instancia de vCenter Server Appliance se puede alojar en el clúster. Durante la etapa 1 de la implementación, al seleccionar un almacén de datos, haga clic en **Instalar en un clúster de vSAN nuevo que contenga el host de destino**. Siga los pasos del asistente del instalador para completar la implementación.

El instalador de vCenter Server Appliance crea un clúster de vSAN de un solo host, y los discos se reclaman desde el host. vCenter Server Appliance se implementa en el clúster de vSAN.

Después de completar la implementación, es posible administrar el clúster de vSAN de host único con la instancia de vCenter Server Appliance. Es necesario completar la configuración del clúster de vSAN.

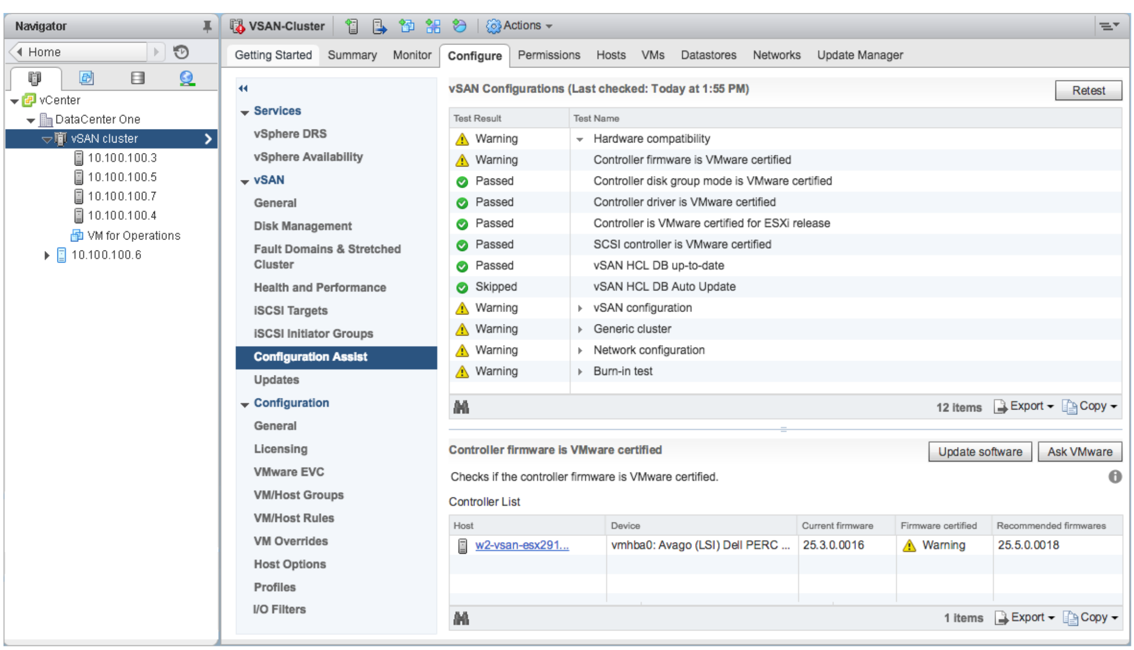
Platform Services Controller y vCenter Server se pueden implementar en el mismo clúster de vSAN o en clústeres distintos.

- Platform Services Controller y vCenter Server se pueden implementar en el mismo clúster de vSAN. Implemente PSC y vCenter Server en el mismo almacén de datos de vSAN de host único. Después de completar la implementación, Platform Services Controller y vCenter Server se ejecutan en el mismo clúster.
- Platform Services Controller y vCenter Server se pueden implementar en distintos clústeres de vSAN. Implemente Platform Services Controller y vCenter Server en distintos clústeres de vSAN de host único. Después de completar la implementación, es necesario completar la configuración de cada clúster de vSAN por separado.

Usar las actualizaciones y el asistente de configuración de vSAN

Es posible utilizar el asistente de configuración para comprobar la configuración del clúster de vSAN y resolver cualquier problema.

El asistente de configuración de vSAN permite verificar la configuración de los componentes del clúster, así como resolver y solucionar problemas. Las comprobaciones de configuración abarcan las opciones de compatibilidad de hardware, red y configuración de vSAN.



Las comprobaciones del asistente de configuración se dividen en dos categorías. Cada categoría contiene comprobaciones de configuración individuales.

Tabla 5-3. Categorías del asistente de configuración

Categoría de configuración	Descripción
Compatibilidad de hardware	Comprueba los componentes de hardware del clúster de vSAN para garantizar que se utilicen el hardware, el software y los controladores admitidos.
Configuración de vSAN	Comprueba las opciones de configuración de vSAN.
Clúster genérico	Comprueba las opciones de configuración básicas del clúster.
Configuración de red	Comprueba la configuración de red de vSAN.
Prueba de grabación	Comprueba las operaciones de prueba de grabación.

Si los controladores o el firmware de la controladora de almacenamiento no cumplen con los requisitos enumerados en la *Guía de compatibilidad de VMware*, se puede utilizar la página Updates (Actualizaciones) para actualizar las controladoras.

Comprobar la configuración de vSAN

Es posible ver el estado de la configuración del clúster de vSAN y resolver problemas que afecten al funcionamiento del clúster.

Procedimiento

1. Desplácese hasta el clúster de vSAN en vSphere Web Client.
2. Haga clic en la pestaña **Configuration** (Configuración).
3. En **vSAN**, haga clic en **Asistente de configuración** para revisar las categorías de configuración de vSAN.

   Si la columna Test Result (Resultado de la prueba) muestra un icono de advertencia, expanda la categoría para examinar los resultados de las comprobaciones de configuración individuales.
4. Seleccione una comprobación de configuración individual y examine la información detallada en la parte inferior de la página.

   Puede hacer clic en el botón **Ask VMware** (Preguntar a VMware) para abrir un artículo de la base de conocimientos donde se describa la comprobación y se proporcione información sobre la forma de resolver el problema.

   En algunas comprobaciones de configuración, se proporcionan botones adicionales para completar la configuración.

Configurar el conmutador distribuido para vSAN

Es posible usar el asistente Configurar nuevo conmutador distribuido para vSAN para configurar una instancia de vSphere Distributed Switch para admitir el tráfico de vSAN.

Si el clúster no dispone de una instancia de vSphere Distributed Switch configurada para admitir el tráfico de vSAN, se muestra una advertencia en la página Asistente de configuración para **Configuración de red > Utilizar vDS para vSAN**.

Procedimiento

1. Desplácese hasta el clúster de vSAN en vSphere Web Client.
2. Haga clic en la pestaña **Configurar**.
3. En vSAN, seleccione **Configuration Assist** (Asistente de configuración) y haga clic para expandir la categoría **Network configuration** (Configuración de red).

4 Haga clic en **Use vDS for vSAN** (Usar vDS para vSAN). En la mitad inferior de la página, haga clic en **Create vDS** (Crear vDS).

5 En Name (Nombre) y Type (Tipo), introduzca un nombre para el nuevo conmutador distribuido y seleccione si desea crear un conmutador nuevo o migrar un conmutador estándar existente.

6 Seleccione los adaptadores sin usar que desea migrar al nuevo conmutador distribuido y haga clic en **Next** (Siguiente).

7 (Opcional) En Migrate infrastructure VMs (Migrar máquinas virtuales de infraestructura), seleccione la máquina virtual que desea tratar como máquina virtual de infraestructura durante la migración del conmutador estándar existente y haga clic en **Next** (Siguiente).

   Este paso no es necesario si desea crear un conmutador distribuido nuevo.

8 En Ready to complete (Listo para completar), revise la configuración y haga clic en **Finish** (Finalizar).

Crear adaptador de red de VMkernel para vSAN

Es posible usar el asistente Nuevos adaptadores de red de VMkernel para vSAN para configurar vmknics que admitan el tráfico de vSAN.

Si los hosts ESXi del clúster no contienen vmknics configuradas para admitir el tráfico de vSAN, se muestra una advertencia en la página Asistente de configuración para **Configuración de red > Todos los hosts tienen una vmknic de vSAN configurada**.

Procedimiento

1 Desplácese hasta el clúster de vSAN en vSphere Web Client.

2 Haga clic en la pestaña **Configurar**.

3 En vSAN, seleccione **Configuration Assist** (Asistente de configuración) y haga clic para expandir la categoría **Network configuration** (Configuración de red).

4 Haga clic en **All hosts have a vSAN vmknic configured** (Todos los hosts tienen una vmknic de vSAN configurada). En la mitad inferior de la página, haga clic en **Create VMkernel Network Adapter** (Crear un adaptador de red de VMkernel).

5 En Seleccionar hosts, active la casilla de cada host que no tenga una vmknic configurada para vSAN y haga clic en **Siguiente**.

   Los hosts sin una vmknic de vSAN se enumerarán en la página Asistente de configuración.

6 En Location and services (Ubicación y servicios), seleccione un conmutador distribuido y active la casilla **vSAN traffic** (Tráfico de vSAN). Haga clic en **Next** (Siguiente).

7 En la configuración del adaptador de vSAN, seleccione un grupo de puertos, las opciones y los ajustes de IP, y haga clic en **Next** (Siguiente).

8 En Ready to complete (Listo para completar), revise la configuración y haga clic en **Finish** (Finalizar).

Instalar las herramientas de administración de controladoras para la actualización de controladores y firmware

Los proveedores de controladoras de almacenamiento ofrecen una herramienta de administración de software que vSAN puede usar para actualizar el firmware y los controladores de controladoras. Si los hosts ESXi no incluyen la herramienta de administración, es posible descargarla.

La página Updates (Actualizaciones) solo admite modelos específicos de controladoras de almacenamiento de ciertos proveedores.

Prerequisitos

- Compruebe la compatibilidad de hardware en la página Configuration Assist (Asistente de configuración).
- DRS debe estar habilitado para poder mantener las máquinas virtuales en ejecución durante las actualizaciones de software.

Procedimiento

1 Desplácese hasta el clúster de vSAN en vSphere Web Client.

2 Haga clic en la pestaña **Configuration** (Configuración).

3 En vSAN, haga clic en **Updates** (Actualizaciones) para revisar los componentes que faltan o están listos para la instalación.

4 Seleccione la herramienta de administración (Mgmt) para la controladora y haga clic en el icono **Download** (Descargar).

La herramienta de administración se descarga de Internet a la instancia de vCenter Server.

5 Haga clic en el icono **Update All** (Actualizar todo) para instalar la herramienta de administración en los hosts ESXi del clúster.

Confirme si desea actualizar todos los hosts a la vez o si prefiere usar una actualización gradual.

6 Haga clic en el icono **Refresh** (Actualizar).

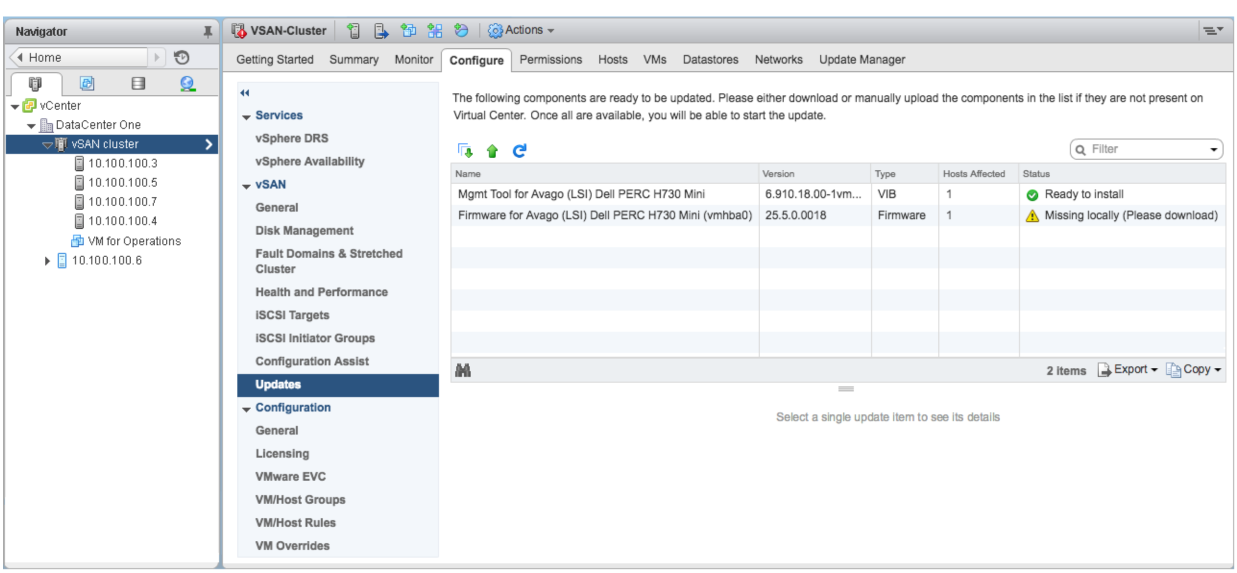
En la página Updates (Actualizaciones), se muestran los componentes de la controladora que requieren una actualización.

Qué hacer a continuación

Cuando la herramienta de administración de controladoras de almacenamiento está disponible, en la página Updates (Actualizaciones), figuran el firmware o los controladores faltantes. Puede actualizar los componentes que faltan.

Actualizar el firmware y los controladores de la controladora de almacenamiento

Puede usar vSAN para actualizar el firmware y los controladores antiguos o incorrectos en las controladoras de almacenamiento.



El asistente de configuración comprueba que las controladoras de almacenamiento usen la versión de controlador y firmware más reciente de acuerdo con la *Guía de compatibilidad de VMware*. Si el firmware o los controladores de controladora no cumplen con los requisitos, puede actualizarlos desde la página Updates (Actualizaciones).

Prerequisitos

Las herramientas de administración de controladoras de los dispositivos de almacenamiento deben estar presentes en el host ESXi.

Procedimiento

1 Desplácese hasta el clúster de vSAN en vSphere Web Client.

2 Haga clic en la pestaña **Configuration** (Configuración).

3 En vSAN, haga clic en **Updates** (Actualizaciones) para revisar los componentes que faltan o están listos para la instalación.

   En la página Updates (Actualizaciones), se muestran los componentes de controlador o firmware faltantes.

   NOTA: Si la herramienta de administración (Mgmt) no está disponible, se le pedirá que descargue e instale la herramienta de administración. Cuando la herramienta esté disponible, se mostrarán el firmware o los controladores faltantes.

4 Seleccione el componente que desea actualizar y haga clic en el icono **Update** (Actualizar) para actualizar el componente en los hosts ESXi del clúster. Como opción, puede hacer clic en el icono **Update All** (Actualizar todo) para actualizar todos los componentes que faltan.

   Confirme si desea actualizar todos los hosts a la vez o si prefiere usar una actualización gradual.

   NOTA: En el caso de algunos controladores y ciertas herramientas de administración, el proceso de actualización omite el modo de mantenimiento y se ejecuta un reinicio basado en el resultado de la instalación. En estos casos, los campos **MM Required** (MM requerido) y **Reboot Required** (Reinicio requerido) están vacíos.

5 Haga clic en el icono **Refresh** (Actualizar).

   Los componentes actualizados no aparecen en la pantalla.

Extender un almacén de datos a dos sitios con clústeres ampliados

6

Es posible crear un clúster ampliado que abarque dos ubicaciones geográficas (o sitios). Los clústeres ampliados permiten extender el almacén de datos de vSAN a dos sitios para utilizarlo como almacenamiento ampliado. El clúster ampliado continúa funcionando si se produce un error o se realizan tareas de mantenimiento programadas en un sitio.

Este capítulo cubre los siguientes temas:

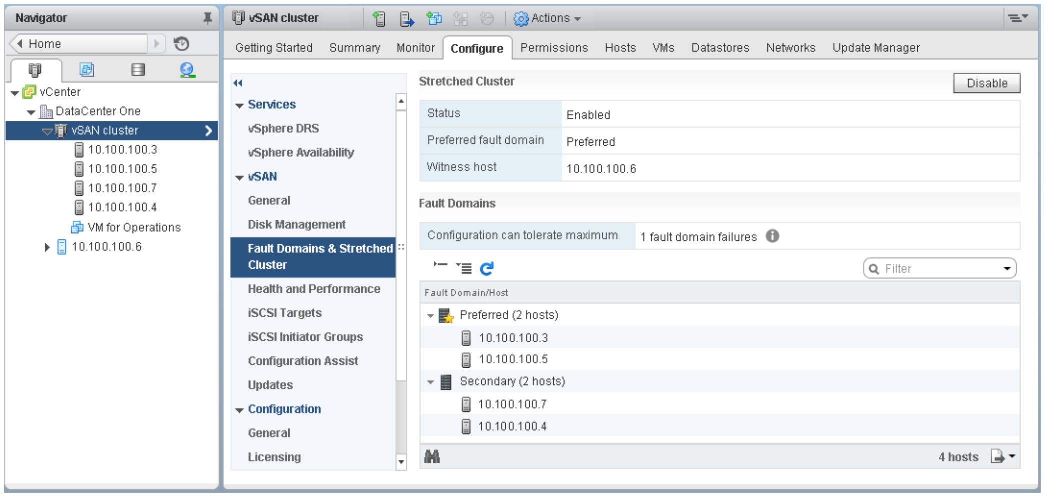
Introducción a los clústeres ampliados

Los clústeres ampliados extienden el clúster de vSAN de un solo sitio a dos sitios para obtener un mayor nivel de disponibilidad y de equilibrio de carga entre sitios. Los clústeres ampliados en general se implementan en entornos donde la distancia entre los centros de datos es limitada, por ejemplo, entornos metropolitanos o de campus.

Los clústeres ampliados se pueden utilizar para administrar el mantenimiento planificado y evitar situaciones problemáticas, ya que el mantenimiento o la pérdida de un sitio no afectan la operación general del clúster. En la configuración de un clúster ampliado, los dos sitios son sitios activos. Si uno de los sitios tiene errores, vSAN usa el almacenamiento del otro sitio. vSphere HA reinicia las máquinas virtuales que deben reiniciarse en el sitio activo restante.

Debe designar un sitio como el sitio preferido. El otro sitio es el secundario o no preferido. El sistema utiliza el sitio preferido solo cuando existe una pérdida de conexión entre los dos sitios activos, así que el sitio designado como preferido es el que se mantiene operativo.

Un clúster ampliado de vSAN puede tolerar un error de vínculo por vez sin perder la disponibilidad de los datos. Un error de vínculo es una pérdida de conexión de red entre los dos sitios o entre un sitio y el host testigo. Durante el error de un sitio o la pérdida de conexión de red, vSAN cambia de manera automática a sitios funcionales en su totalidad.



Para obtener más información sobre el trabajo con clústeres ampliados, consulte la *guía de clúster ampliado de vSAN*.

Host testigo

Cada clúster ampliado está formado por dos sitios y un host testigo. El host testigo reside en un tercer sitio y contiene los componentes testigo de los objetos de la máquina virtual. Solo contiene metadatos, y no participa de las operaciones de almacenamiento.

El host testigo sirve como factor determinante cuando se debe tomar una decisión en relación con la disponibilidad de los componentes del almacén de datos cuando se pierde la conexión de red entre dos sitios. En este caso, el host testigo por lo general forma un clúster de vSAN con el sitio preferido. Pero si el sitio preferido queda aislado del sitio secundario y del testigo, el host testigo forma un clúster con el sitio secundario. Una vez que el sitio preferido está conectado nuevamente, se vuelven a sincronizar los datos para garantizar que ambos sitios posean las copias más recientes de todos los datos.

Si se produce un error en el host testigo, todos los objetos correspondientes dejan de ser compatibles, pero se puede acceder a ellos en su totalidad.

El host testigo tiene las siguientes características:

- El host testigo puede utilizar vínculos de poco ancho de banda/latencia alta.
- El host testigo no puede ejecutar máquinas virtuales.
- Un solo host testigo admite solamente un clúster ampliado de vSAN.
- El host testigo debe tener un adaptador de VMkernel con tráfico de vSAN habilitado y conexiones a todos los hosts del clúster. El host testigo usa un adaptador de VMkernel para la administración y otro adaptador de VMkernel para el tráfico de datos de vSAN. El host testigo solo puede tener un adaptador de VMkernel dedicado a vSAN.
- El host testigo debe ser un host independiente dedicado al clúster ampliado. No se puede agregar a ningún otro clúster ni mover en el inventario mediante vCenter Server.

El host testigo puede ser un host físico o un host ESXi que se ejecuta en una máquina virtual. El host testigo de máquina virtual no proporciona otro tipo de funcionalidad, como almacenamiento o ejecución de máquinas virtuales. Se pueden ejecutar varios hosts testigo como máquinas virtuales en un solo servidor físico. En el caso de las revisiones y la configuración básica de redes y supervisión, el host testigo de máquina virtual funciona de la misma forma que lo hace un host ESXi típico. Puede administrarlo con vCenter Server, aplicar revisiones y actualizaciones mediante `esxcli` o vSphere Update Manager, y supervisarlo con herramientas estándar que interactúen con hosts ESXi.

Puede usar un dispositivo virtual testigo como host testigo en un clúster ampliado. El dispositivo virtual testigo es un host ESXi en una máquina virtual, empaquetado como OVF u OVA. El dispositivo está disponible en varias opciones, según el tamaño de la implementación.

Clúster ampliado versus dominios de errores

Los clústeres ampliados proporcionan protección contra redundancias y errores entre los centros de datos de dos ubicaciones geográficas. Los dominios de errores brindan protección contra errores en el nivel del gabinete dentro del mismo sitio. Cada sitio de un clúster ampliado reside en un dominio de errores distinto.

Un clúster ampliado requiere tres dominios de errores: el sitio preferido, el sitio secundario y el host testigo.

En vSAN 6.6 y en versiones posteriores, es posible ofrecer un nivel adicional de protección contra errores locales para los objetos de máquinas virtuales en clústeres ampliados. Al configurar un clúster ampliado con cuatro o más hosts en cada sitio, están disponibles las siguientes reglas de directivas para los objetos del clúster:

- **Nivel primario de errores que se toleran (Primary level of failures to tolerate, PFTT)**. Esta regla define el número de errores de dispositivos y hosts que se pueden tolerar en un objeto de una máquina virtual en los dos sitios. El valor predeterminado es 1 y el máximo es 3.
- **Nivel secundario de errores que se toleran**. Define el número de errores de dispositivos y hosts que se pueden tolerar en un objeto de una máquina virtual en un solo sitio. El valor predeterminado es 0 y el máximo es 3.
- **Compatibilidad**. Esta regla solo se encuentra disponible si **Primary level of failures to tolerate** (Nivel primario de errores que se toleran) se configura en 0. Es posible configurar la regla de compatibilidad en None (Ninguno), Preferred (Preferido) o Secondary (Secundario). Esta regla permite limitar los objetos de una máquina virtual a un sitio seleccionado en el clúster ampliado. El valor predeterminado es None (Ninguno).

NOTA: Al configurar el valor de **Secondary level of failures to tolerate** (Nivel secundario de errores que se toleran) para el clúster ampliado, se aplica la regla del **Método de tolerancia a errores** en el **nivel secundario**. El método de tolerancia a errores que se utiliza para el **PFTT** se establece de manera predeterminada en RAID 1.

En un clúster ampliado con protección contra errores locales, el clúster puede ejecutar reparaciones de los componentes faltantes o dañados en el sitio disponible, incluso cuando un sitio no está disponible.

Consideraciones de diseño para clústeres ampliados

Tenga en cuenta las siguientes directrices cuando trabaje con un clúster ampliado de vSAN.

- Configure las opciones de DRS para el clúster ampliado.
  - DRS debe estar habilitado en el clúster. Si DRS se coloca en el modo parcialmente automatizado, se puede controlar qué máquinas virtuales se deben migrar a cada sitio.
  - Cree dos grupos de hosts, uno para el sitio preferido y otro para el sitio secundario.
  - Cree dos grupos de máquinas virtuales, uno para mantener las máquinas virtuales en el sitio preferido y otro para mantener las máquinas virtuales en el sitio secundario.

  - Cree dos reglas de afinidad de máquina virtual-host para asignar máquinas virtuales a grupos de hosts, y especifique qué máquinas virtuales y hosts residen en el sitio preferido y qué máquinas virtuales y hosts residen en el sitio secundario.
  - Configure reglas de afinidad de máquina virtual-host para realizar la colocación inicial de las máquinas virtuales en el clúster.
- Configure las opciones de HA para el clúster ampliado.
  - HA debe estar habilitado en el clúster.
  - La configuración de la regla de HA debe respetar las reglas de afinidad de máquina virtual-host durante la conmutación por error.
  - Deshabilite los latidos de almacén de datos de HA.
- Los clústeres ampliados requieren un formato en disco 2.0 o posterior. Si es necesario, actualice el formato en disco antes de configurar un clúster ampliado. Consulte "Actualizar el formato de disco de vSAN mediante vSphere Web Client," página 102.
- Configure el valor de **Primary level of failures to tolerate** (Nivel primario de errores que se toleran) en 1 para los clústeres ampliados.
- Los clústeres ampliados de vSAN no admiten Fault Tolerance con multiprocesador simétrico (SMP-FT).
- Cuando un host se desconecta o no responde, no se puede agregar ni quitar el host testigo. Esta limitación garantiza que vSAN recopile suficiente información de todos los hosts antes de iniciar las operaciones de reconfiguración.
- No se admite el uso de `esxcli` para agregar o quitar hosts de clústeres ampliados.

Prácticas recomendadas para trabajar con clústeres ampliados

Cuando trabaje con clústeres ampliados de vSAN, siga estas recomendaciones para obtener un rendimiento apropiado.

- Aún si no se puede acceder a uno de los sitios (dominios de errores) de un clúster ampliado, se pueden aprovisionar nuevas máquinas virtuales en el subclúster que contiene los otros dos sitios. Estas máquinas virtuales nuevas se aprovisionan en forma forzada e implícita y no serán compatibles hasta que el sitio particionado vuelva a unirse al clúster. El aprovisionamiento en forma forzada e implícita se realiza solo cuando dos de los tres sitios están disponibles. Un sitio aquí se refiere tanto a un sitio de datos como al host testigo.
- Si un sitio entero queda sin conexión debido a un corte de suministro eléctrico o a una pérdida de conexión de red, reinicie el sitio inmediatamente, sin demorarse mucho. En lugar de reiniciar los hosts de vSAN uno por uno, conecte todos los hosts casi al mismo tiempo, idealmente dentro de un lapso de 10 minutos. Al seguir este proceso, evita la resincronización de gran cantidad de datos entre los sitios.
- Si un host no está disponible en forma permanente, quite el host del clúster antes de realizar tareas de reconfiguración.
- Si desea clonar un host testigo de máquina virtual para que admita varios clústeres ampliados, no configure la máquina virtual como host testigo antes de clonarla. Primero, implemente la máquina virtual desde el archivo de OVF; después, clone la máquina virtual y, por último, configure cada clon como host testigo para un clúster diferente. O bien puede implementar tantas máquinas virtuales como necesite desde el archivo de OVF y configurar cada una como host testigo para un clúster diferente.

Diseño de red para clústeres ampliados

Los tres sitios en un clúster ampliado se comunican en la red de administración y la red de vSAN. Las máquinas virtuales en los dos sitios de datos se comunican en una red de máquina virtual común.

Un clúster ampliado de vSAN debe cumplir con ciertos requisitos básicos de red.

- La red de administración requiere conectividad entre los tres sitios, mediante una red ampliada de Capa 2 o una red de Capa 3.
- La red de vSAN requiere conectividad entre los tres sitios. VMware recomienda utilizar una red ampliada de Capa 2 entre los dos sitios de datos y una red de Capa 3 entre los sitios de datos y el host testigo.
- La red de máquina virtual requiere conectividad entre los sitios de datos, pero no el host testigo. VMware recomienda utilizar una red ampliada de Capa 2 entre los sitios de datos. En caso de que se produzca un error, las máquinas virtuales no requieren una dirección IP nueva para funcionar en el sitio remoto.
- La red de vMotion requiere conectividad entre los sitios de datos, pero no el host testigo. VMware admite el uso de una red ampliada de Capa 2 o una red de Capa 3 entre los sitios de datos.

Uso de rutas estáticas en hosts de ESXi

Si utiliza una sola puerta de enlace predeterminada en los hosts ESXi, tenga en cuenta que cada host ESXi contiene una pila de TCP/IP predeterminada que posee una única puerta de enlace predeterminada. Por lo general, la ruta predeterminada se asocia con la pila de TCP/IP de la red de administración.

Es posible que la red de administración y la red de vSAN estén separadas una de otra. Por ejemplo, la red de administración puede usar vmk0 en una NIC física 0, mientras que la red de vSAN puede usar vmk2 en una NIC física 1 (adaptadores de red distintos para dos pilas de TCP/IP diferentes). Esta configuración implica que la red de vSAN no posee una puerta de enlace predeterminada.

Considere una red de vSAN que abarca dos sitios de datos en un dominio de difusión de Capa 2 (por ejemplo, 172.10.0.0) y el host testigo se encuentra en otro dominio de difusión (por ejemplo, 172.30.0.0). Si los adaptadores de VMkernel de un sitio de datos intentan conectarse a la red de vSAN en el host testigo, se producirán errores en la conexión, ya que la puerta de enlace predeterminada en el host ESXi está asociada a la red de administración y no existe una ruta desde la red de administración hacia la red de vSAN.

Se pueden usar rutas estáticas para solucionar este problema. Defina una nueva entrada de enrutamiento que indique qué ruta seguir para alcanzar una red en particular. Para una red de vSAN en un clúster ampliado es posible agregar rutas estáticas para garantizar una comunicación apropiada entre los hosts.

Por ejemplo, se puede agregar una ruta estática a los hosts en cada sitio de datos, de modo que las solicitudes que deben llegar a la red testigo 172.30.0.0 se enruten mediante la interfaz 172.10.0.0. También se puede agregar una ruta estática al host testigo, de modo que las solicitudes que deben llegar a la red 172.10.0.0 para los sitios de datos se enruten mediante la interfaz 172.30.0.0.

NOTA: Si utiliza rutas estáticas, debe agregar de manera manual las rutas estáticas para los hosts ESXi nuevos que se agreguen a alguno de los sitios a fin de que esos hosts puedan comunicarse en todo el clúster. Si reemplaza el host testigo, debe actualizar la configuración de la ruta estática.

Use el comando `esxcli network ip route` para agregar rutas estáticas.

Configurar el clúster ampliado de vSAN

Configure un clúster de vSAN que abarque dos sitios o ubicaciones geográficas.

Prerequisitos

- Compruebe que dispone de un mínimo de tres hosts: uno para el sitio preferido, uno para el sitio secundario y un host para que funcione como testigo.
- Asegúrese de haber configurado un host para que sirva como host testigo para el clúster ampliado. Compruebe que el host testigo no forme parte del clúster de vSAN, y que solo haya un adaptador de VMkernel configurado para el tráfico de datos de vSAN.
- Asegúrese de que el host testigo esté vacío y no contenga ningún componente. Para configurar un host vSAN como host testigo, primero evacúe los datos del host y elimine el grupo de discos.

Procedimiento

1. Desplácese hasta el clúster de vSAN en vSphere Web Client.
2. Haga clic en la pestaña **Configurar**.
3. En vSAN, haga clic en **Fault Domains and Stretched Cluster** (Dominios de errores y clúster ampliado).
4. Haga clic en el botón **Configure** (Configurar) para clúster ampliado para abrir el asistente de configuración de clúster ampliado.
5. Seleccione el dominio de errores que desea asignar al sitio secundario y haga clic en **>>**.

   Los hosts que se enumeran debajo del dominio de errores preferido se encuentran en el sitio preferido.
6. Haga clic en **Next** (Siguiente).
7. Seleccione un host testigo que no sea miembro del clúster ampliado de vSAN y haga clic en **Siguiente**.
8. Reclame los dispositivos de almacenamiento en el host testigo y haga clic en **Next** (Siguiente).

   Reclame los dispositivos de almacenamiento en el host testigo. Seleccione un dispositivo flash para el nivel de memoria caché y uno o más dispositivos para el nivel de capacidad.
9. En la página Ready to complete (Listo para finalizar), revise la configuración y haga clic en **Finish** (Finalizar).

Cambiar el dominio de errores preferido

Es posible configurar el sitio secundario como el sitio preferido. El sitio preferido actual se convierte en el sitio secundario.

Procedimiento

1. Desplácese hasta el clúster de vSAN en vSphere Web Client.
2. Haga clic en la pestaña **Configurar**.
3. En vSAN, haga clic en **Fault Domains and Stretched Cluster** (Dominios de errores y clúster ampliado).
4. Seleccione el dominio de errores secundario y haga clic en el icono **Mark Fault Domain as preferred for Stretched Cluster** (Marcar dominio de errores como preferido para un clúster ampliado) ().
5. Haga clic en **Yes** (Sí) para confirmar.

   El dominio de errores seleccionado se marca como el dominio de errores preferido.

Cambiar el host testigo

Es posible cambiar el host testigo de un clúster ampliado de vSAN.

Cambie el host ESXi usado como host testigo del clúster ampliado de vSAN.

Prerequisitos

Compruebe que el host testigo no esté en uso.

Procedimiento

1. Desplácese hasta el clúster de vSAN en vSphere Web Client.
2. Haga clic en la pestaña **Configurar**.
3. En vSAN, haga clic en **Dominios de errores y clúster ampliado**.
4. Haga clic en el botón **Change witness host** (Cambiar host testigo).
5. Seleccione un nuevo host para utilizarlo como host testigo y haga clic en **Next** (Siguiente).
6. Reclame discos en el nuevo host testigo y haga clic en **Next** (Siguiente).
7. En la página Ready to complete (Listo para completar), revise la configuración y haga clic en **Finish** (Finalizar).

Implementar un dispositivo testigo de vSAN

Ciertas configuraciones de vSAN, como los clústeres ampliados, requieren un host testigo. En lugar de usar un host de ESXi físico dedicado como host testigo, puede implementar el dispositivo testigo de vSAN. El dispositivo es una máquina virtual preconfigurada que se ejecuta en ESXi y se distribuye como un archivo OVA.

Al contrario que los hosts de ESXi de uso genérico, el dispositivo testigo no ejecuta máquinas virtuales. Su único propósito es funcionar como testigo de vSAN.

El flujo de trabajo para implementar y configurar el dispositivo testigo de vSAN incluye este proceso.

1. Descargue el dispositivo del sitio web de VMware.
2. Implemente el dispositivo en un host o un clúster de vSAN. Para obtener más información, consulte Implementar plantillas OVF en la documentación de *Administrar máquinas virtuales de vSphere*.
3. Configure la red de vSAN en el dispositivo testigo.
4. Configure la red de administración de en el dispositivo testigo.
5. Agregue el dispositivo a vCenter Server como un host testigo de ESXi. Asegúrese de configurar la interfaz de VMkernel de vSAN en el host.

Configurar la red de vSAN en el dispositivo testigo

El dispositivo testigo de vSAN incluye dos adaptadores de red preconfigurados. Debe cambiar la configuración del segundo adaptador de modo que el dispositivo se pueda conectar a la red de vSAN.

Procedimiento

1. En el vSphere Web Client, desplácese hasta el dispositivo virtual que contenga el host testigo.
2. Haga clic con el botón derecho en el dispositivo y seleccione **Editar configuración**.
3. En la pestaña **Hardware virtual**, expanda el segundo adaptador de red.
4. En el menú desplegable, seleccione el grupo de puertos de vSAN y haga clic en **Aceptar**.

Configurar la red de administración

Configure el dispositivo testigo de modo que se pueda acceder a él en la red.

De forma predeterminada, el dispositivo puede obtener automáticamente los parámetros de red si esta incluye un servidor DHCP. Si no es así, debe configurar los ajustes correspondientes.

Procedimiento

1 Encienda el dispositivo testigo y abra su consola.

  Debido a que el dispositivo es un host de ESXi, verá la interfaz de usuario de consola directa (DCUI).

2 Pulse F2 y desplácese hasta la página Adaptadores de red.

3 En la página Adaptadores de red, compruebe que se haya seleccionado al menos un vmnic para el transporte.

4 Configure los parámetros de IPv4 para la red de administración.

   a Desplácese hasta la sección Configuración de IPv4 y cambie el ajuste predeterminado de DHCP a estático.

   b Introduzca los siguientes ajustes:

      - Dirección IP
      - Máscara de subred
      - Puerta de enlace predeterminada

5 Configure los parámetros de DNS.

   - Servidor DNS principal
   - Servidor DNS alternativo
   - Nombre de host

Configurar la interfaz de red para el tráfico testigo

El tráfico de datos de vSAN requiere un vínculo de latencia baja y ancho de banda alto. El tráfico testigo puede usar un vínculo de latencia baja, ancho de banda alto y que se pueda enrutar. Para separar el tráfico de datos del tráfico testigo, puede configurar un adaptador de red de VMkernel dedicado para el tráfico testigo de vSAN.

Puede separar el tráfico de datos del tráfico testigo en las configuraciones de clúster ampliado admitidas. El adaptador de VMkernel utilizado para el tráfico de datos de vSAN y el adaptador de VMkernel utilizado para el tráfico testigo se deben conectar al mismo conmutador físico.

Puede agregar compatibilidad a una conexión cruzada de red directa con el objetivo de transferir el tráfico de datos de vSAN en un clúster ampliado de vSAN de dos hosts. Puede configurar una conexión de red independiente para el tráfico testigo. En cada host de datos del clúster, configure el adaptador de red de VMkernel de administración para que también transfiera el tráfico testigo. No configure el tipo de tráfico testigo en el host testigo.

Prerequisitos

- Compruebe que la conexión entre el sitio de datos y el tráfico testigo tenga un ancho de banda mínimo de 100 MBps, y una latencia de menos de 200 ms de RTT.
- Compruebe que el tráfico de vSAN se puede transferir a través de una conexión directa mediante cable Ethernet con una velocidad de 10 GBps.
- Compruebe que el tráfico de datos y el tráfico testigo usen la misma versión de IP.

Procedimiento

1 Abra una conexión de SSH para el host ESXi.

2 Use el comando `esxcli network ip interface list` para determinar el adaptador de red de VMkernel que se usará para el tráfico de administración.

Por ejemplo:

```
esxcli network  ip interface list
vmk0
   Name: vmk0
   MAC Address: e4:11:5b:11:8c:16
   Enabled: true
   Portset: vSwitch0
   Portgroup: Red de administración
   Netstack Instance: defaultTcpipStack
   VDS Name: N/A
   VDS UUID: N/A
   VDS Port: N/A
   VDS Connection: -1
   Opaque Network ID: N/A
   Opaque Network Type: N/A
   External ID: N/A
   MTU: 1500
   TSO MSS: 65535
   Port ID: 33554437

vmk1
   Name: vmk1
   MAC Address: 00:50:56:6a:3a:74
   Enabled: true
   Portset: vSwitch1
   Portgroup: vsandata
   Netstack Instance: defaultTcpipStack
  VDS Name: N/A
   VDS UUID: N/A
   VDS Port: N/A
   VDS Connection: -1
   Opaque Network ID: N/A
   Opaque Network Type: N/A
   External ID: N/A
   MTU: 9000
   TSO MSS: 65535
   Port ID: 50331660
```

NOTA: Se incluye información de multidifusión para la compatibilidad con versiones anteriores. vSAN 6.6 y las versiones posteriores no requieren multidifusión.

3 Use el comando `esxcli vsan network ip add` para configurar el adaptador de red de VMkernel de administración y admitir el tráfico testigo.

```
esxcli vsan network ip add -i vmkx -T=witness
```

4 Use el comando `esxcli vsan network list` para comprobar la nueva configuración de red.

Por ejemplo:

```
esxcli vsan network list
Interface
   VmkNic Name: vmk0
   IP Protocol: IP
   Interface UUID: 8cf3ec57-c9ea-148b-56e1-a0369f56dcc0
   Agent Group Multicast Address: 224.2.3.4
   Agent Group IPv6 Multicast Address: ff19::2:3:4
   Agent Group Multicast Port: 23451
   Master Group Multicast Address: 224.1.2.3
   Master Group IPv6 Multicast Address: ff19::1:2:3
   Master Group Multicast Port: 12345
   Host Unicast Channel Bound Port: 12321
   Multicast TTL: 5
   Traffic Type: testigo

Interface
   VmkNic Name: vmk1
   IP Protocol: IP
   Interface UUID: 6df3ec57-4fb6-5722-da3d-a0369f56dcc0
   Agent Group Multicast Address: 224.2.3.4
   Agent Group IPv6 Multicast Address: ff19::2:3:4
   Agent Group Multicast Port: 23451
   Master Group Multicast Address: 224.1.2.3
   Master Group IPv6 Multicast Address: ff19::1:2:3
   Master Group Multicast Port: 12345
   Host Unicast Channel Bound Port: 12321
   Multicast TTL: 5
   Traffic Type: vsan
```

En vSphere Web Client, la interfaz de red de VMkernel de administración no se selecciona para el tráfico de vSAN. No vuelva a habilitar la interfaz en vSphere Web Client.

Convertir un clúster ampliado en un clúster estándar de vSAN

Puede retirar un clúster ampliado y convertirlo en un clúster estándar de vSAN.

Cuando se deshabilita un clúster ampliado, se elimina el host testigo, pero se conserva la configuración del dominio de errores. Debido a que el host testigo no está disponible, no habrá componentes testigo para las máquinas virtuales. Para garantizar la disponibilidad completa para las máquinas virtuales, repare los objetos de clúster de forma inmediata.

Procedimiento

1 Desplácese hasta el clúster ampliado de vSAN en vSphere Web Client.

2 Deshabilite el clúster ampliado.

   a Haga clic en la pestaña **Configurar**.

   b En vSAN, haga clic en **Fault Domains and Stretched Cluster** (Dominios de errores y clúster ampliado).

   c Haga clic en el botón **Configurar** del clúster ampliado.

   Se abrirá el asistente para la configuración del clúster ampliado.

   d Haga clic en **Deshabilitar** y, a continuación, en **Sí** para confirmar.

3 Elimine la configuración de dominio de errores.

   a Seleccione un dominio de errores y haga clic en el icono **Quitar dominios de errores seleccionados** (). Haga clic en **Yes** (Sí) para confirmar.

   b Seleccione el otro dominio de errores y haga clic en el icono **Quitar dominios de errores seleccionados** (). Haga clic en **Yes** (Sí) para confirmar.

4 Repare los objetos del clúster.

   a Haga clic en la pestaña **Supervisar** y seleccione **vSAN**.

   b En vSAN, haga clic en **Estado** y seleccione **Estado de objetos de vSAN**.

   c Haga clic en **Reparar objeto inmediatamente**.

vSAN volverá a crear los componentes testigo en el clúster.

Aumentar la eficiencia de espacio en un clúster de vSAN

7

Puede utilizar las técnicas de eficiencia de espacio para reducir la cantidad de espacio para el almacenamiento de datos. Estas técnicas reducen el espacio de almacenamiento total requerido para satisfacer sus necesidades.

Este capítulo cubre los siguientes temas:

Introducción a la eficiencia de espacio de vSAN

Puede utilizar las técnicas de eficiencia de espacio para reducir la cantidad de espacio para el almacenamiento de datos. Estas técnicas reducen la capacidad de almacenamiento total requerida para satisfacer sus necesidades.

Puede habilitar la desduplicación y compresión en un clúster de vSAN para eliminar los datos duplicados y reducir la cantidad de espacio necesario para almacenar datos.

Puede establecer el atributo de la directiva **Failure tolerance method** (Método de tolerancia ante errores) para utilizar la codificación de borrado RAID 5 o RAID 6. La codificación de borrado puede proteger sus datos y, al mismo tiempo, utilizar menos espacio de almacenamiento que el método de reflejo RAID 1 predeterminado.

Puede utilizar la desduplicación y compresión, y la codificación de borrado RAID 5 o RAID 6 para aumentar los ahorros en espacio de almacenamiento. RAID 5 o RAID 6 proporcionan ahorros de espacio claramente definidos en comparación con RAID 1. La desduplicación y la compresión pueden proporcionar ahorros adicionales.

Uso de la desduplicación y compresión

vSAN puede realizar la desduplicación y compresión a nivel de bloque para ahorrar espacio de almacenamiento. Cuando habilite la desduplicación y compresión en un clúster basado íntegramente en tecnología flash de vSAN, se reducen los datos redundantes dentro de cada grupo de discos.

La desduplicación elimina los bloques de datos redundantes, mientras que la compresión elimina los datos redundantes adicionales dentro de cada bloque de datos. Estas técnicas funcionan en conjunto para reducir la cantidad de espacio requerido para almacenar los datos. vSAN aplica la desduplicación y luego la compresión a medida que traslada los datos desde el nivel de memoria caché al nivel de capacidad.

Puede habilitar la desduplicación y compresión como una configuración integral del clúster, pero se aplican en cada grupo de discos en particular. Cuando habilite la desduplicación y compresión en un clúster de vSAN, se reducen los datos redundantes dentro de un grupo de discos en particular a una sola copia.

Puede habilitar la desduplicación y compresión cuando cree un clúster basado íntegramente en tecnología flash de vSAN nuevo o cuando edite un clúster basado íntegramente en tecnología flash de vSAN existente. Para obtener más información sobre la creación y edición de los clústeres de vSAN, consulte "Habilitar vSAN," página 49.

Cuando habilite o deshabilite la desduplicación y compresión, vSAN realizará un reformateo secuencial de cada grupo de discos de cada host. De acuerdo con los datos almacenados en el almacén de datos de vSAN, este proceso podría demorar bastante tiempo. Se recomienda que no realice estas operaciones de forma frecuente. Si planifica deshabilitar la desduplicación y compresión, deberá verificar en primer lugar que exista suficiente capacidad física para colocar los datos.

NOTA: Puede que la desduplicación y la compresión no sean efectivas para las máquinas virtuales cifradas, ya que el cifrado de las máquinas virtuales cifra los datos del host antes de escribirlos fuera del almacenamiento. Tenga en cuenta los intercambios de almacenamiento cuando use el cifrado de máquinas virtuales.

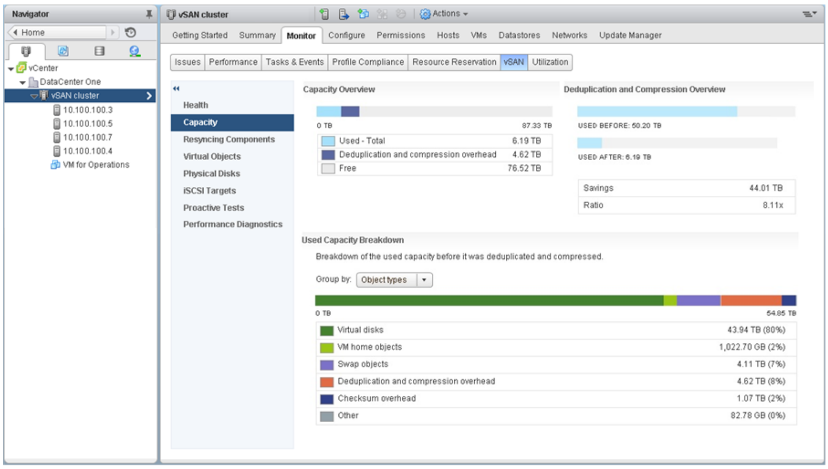
Cómo administrar los discos en un clúster con desduplicación y compresión

Considere las siguientes directrices al administrar discos en un clúster con la desduplicación y compresión habilitadas.

- Evite agregar discos a un grupo de discos de forma incremental. Para una desduplicación y compresión más eficientes, considere agregar un grupo de discos nuevo para aumentar la capacidad de almacenamiento del clúster.
- Cuando agregue un grupo de discos nuevo de forma manual, agregue todos los discos de capacidad al mismo tiempo.
- No es posible eliminar un solo disco de un grupo de discos. Deberá eliminar el grupo de discos entero para realizar modificaciones.
- El error de un solo disco provocará errores en el grupo de discos entero.

Cómo verificar los ahorros de espacio generados por la desduplicación y compresión

La cantidad de reducción de espacio generada por la desduplicación y compresión depende de varios factores, incluido el tipo de datos almacenados y la cantidad de bloques duplicados. Los grupos de discos más grandes tienden a brindar una proporción de desduplicación más elevada. Puede comprobar los resultados de la desduplicación y compresión accediendo a Información general sobre Desduplicación y compresión en Supervisión de capacidad de vSAN.



Puede visualizar la opción Descripción general de desduplicación y compresión cuando supervise la capacidad de vSAN en vSphere Web Client. Muestra información sobre los resultados de la desduplicación y compresión. El espacio Usado antes indica el espacio lógico requerido antes de aplicar la desduplicación y compresión, mientras que el espacio Usado después indica el espacio físico usado después de aplicar la desduplicación y compresión. El espacio Usado después también muestra una descripción general de la cantidad de espacio ahorrado, y la proporción de la desduplicación y compresión.

La proporción de desduplicación y compresión se basa en el espacio Usado antes lógico requerido para almacenar los datos antes de la implementación de la desduplicación y compresión, en relación con el espacio Usado después físico requerido después de aplicar la desduplicación y compresión. Específicamente, la proporción es el espacio Usado antes dividido por el espacio Usado después. Por ejemplo, si el espacio Usado antes es 3 GB, pero el espacio Usado después físico es 1 GB, la proporción de desduplicación y compresión es 3x.

Cuando se habilitan la desduplicación y la compresión en el clúster de vSAN, es posible que las actualizaciones de capacidad demoren varios minutos en aparecer en Supervisión de capacidad, a medida que se va reclamando y reasignando el espacio de disco.

Consideraciones de diseño de desduplicación y compresión

Considere estas directrices al configurar la desduplicación y compresión en un clúster de vSAN.

- La desduplicación y compresión están disponibles solo en grupos de discos basados íntegramente en tecnología flash.
- Se requiere el formato en disco versión 3.0 o posterior para admitir la desduplicación y compresión.
- Deberá tener una licencia válida para poder habilitar la desduplicación y compresión en un clúster.
- Puede habilitar la desduplicación y compresión solo si el método de recuperación de almacenamiento está establecido en manual. Puede cambiar el método de recuperación de almacenamiento a automático después de habilitar la desduplicación y compresión.

- Cuando habilite la desduplicación y compresión en un clúster de vSAN, todos los grupos de discos participarán en la reducción de datos a través de la desduplicación y compresión.
- vSAN puede eliminar los bloques de datos duplicados dentro de cada grupo de discos, pero no entre los grupos de discos.
- La sobrecarga de capacidad para la desduplicación y compresión es aproximadamente un 5 % de la capacidad en bruto total.
- Las directivas deben tener reservas de espacio de objeto del 0 o del 100 %. Las directivas con reservas de espacio de objeto del 100 % siempre se respetan, pero pueden reducir la eficiencia de la desduplicación y la compresión.

Habilitar la desduplicación y la compresión en un nuevo clúster de vSAN

Puede habilitar la desduplicación y la compresión cuando se configura un nuevo clúster basado íntegramente en tecnología flash de vSAN.

Procedimiento

1. Desplácese hasta un clúster existente en vSphere Web Client.
2. Haga clic en la pestaña **Configurar**.
3. En vSAN, seleccione **General** y haga clic en el botón **Configurar vSAN**.
4. Configure la desduplicación y la compresión en el clúster.
   a. En la página **vSAN capabilites** (Funcionalidades de vSAN), marque la casilla **Enable** (Habilitar) en Deduplication and Compression (Desduplicación y compresión).
   b. (Opcional) Habilite la redundancia reducida de las máquinas virtuales.

      Consulte "Reducir la redundancia de la máquina virtual para el clúster de vSAN," página 79.
5. En la página **Reclamar discos**, especifique los discos que se reclamarán para el clúster de vSAN.
   a. Seleccione el dispositivo flash que se utilizará para capacidad y haga clic en el icono **Claim for capacity tier** (Recuperar para nivel de capacidad) ().
   b. Seleccione un dispositivo flash que se utilizará para almacenamiento en caché y haga clic en el icono **Claim for cache tier** (Recuperar para nivel de almacenamiento en caché) ().
6. Complete la configuración del clúster.

Habilitar la desduplicación y la compresión en un clúster de vSAN existente

Puede habilitar la desduplicación y la compresión mediante la edición de los parámetros de configuración de un clúster de vSAN existente.

Prerequisitos

Cree un clúster de vSAN.

Procedimiento

1. Desplácese hasta el clúster del host de vSAN en vSphere Web Client.
2. Haga clic en la pestaña **Configurar**.
3. En vSAN, seleccione **General**.
4. En el panel vSAN está activado, haga clic en el botón **Editar**.

5 Configure la desduplicación y la compresión.

   a Establezca la desduplicación y la compresión como **Habilitado**.

   b (Opcional) Habilite la redundancia reducida de las máquinas virtuales.

   Consulte "Reducir la redundancia de la máquina virtual para el clúster de vSAN," página 79.

   c Haga clic en **OK** (Aceptar) para guardar los cambios realizados en la configuración.

Mientras se habilitan la desduplicación y la compresión, vSAN cambia el formato de disco de todos los grupos de discos del clúster. Para llevar a cabo este cambio, vSAN evacua los datos del grupo de discos, quita el grupo de discos y lo vuelve a crear con un nuevo formato que admite desduplicación y compresión.

La operación de habilitación no requiere migración de máquinas virtuales ni DRS. El tiempo necesario para llevar a cabo esta operación depende de la cantidad de hosts del clúster y de la cantidad de datos. Puede supervisar el progreso en la pestaña **Tareas y eventos**.

Deshabilitar la desduplicación y la compresión

Puede deshabilitar la desduplicación y la compresión en el clúster de vSAN.

Cuando se deshabilitan la desduplicación y la compresión en el clúster de vSAN, se puede expandir el tamaño de la capacidad usada en el clúster (en función de la proporción de desduplicación). Antes de deshabilitar la desduplicación y la compresión, compruebe que el clúster tenga suficiente capacidad para gestionar el tamaño de los datos ampliados.

Procedimiento

1 Desplácese hasta el clúster del host de vSAN en vSphere Web Client.

2 Haga clic en la pestaña **Configurar**.

3 En vSAN, seleccione **General**.

4 En el panel vSAN is turned ON (vSAN está activado), haga clic en el botón **Edit** (Editar).

5 Deshabilite la desduplicación y la compresión.

   a Establezca el modo de reclamo de discos como **Manual**.

   b Establezca la desduplicación y la compresión como **Deshabilitado**.

   c Haga clic en **OK** (Aceptar) para guardar los cambios realizados en la configuración.

Mientras se deshabilitan la desduplicación y la compresión, vSAN cambia el formato de disco de todos los grupos de discos del clúster. Evacua los datos del grupo de discos, quita el grupo de discos y lo vuelve a crear con un formato que no admite desduplicación y compresión.

El tiempo necesario para llevar a cabo esta operación depende de la cantidad de hosts del clúster y de la cantidad de datos. Puede supervisar el progreso en la pestaña **Tareas y eventos**.

Reducir la redundancia de la máquina virtual para el clúster de vSAN

Cuando se habilitan la desduplicación y la compresión, en algunos casos, puede que sea necesario reducir el nivel de protección de las máquinas virtuales.

Habilitar la desduplicación y la compresión requiere un cambio de formato de los grupos de discos. Para llevar a cabo este cambio, vSAN evacua los datos del grupo de discos, quita el grupo de discos y lo vuelve a crear con un nuevo formato que admite desduplicación y compresión.

En algunos entornos, puede que el clúster de vSAN no tenga suficientes recursos para evacuar por completo el grupo de discos. Un ejemplo de dicha implementación puede ser un clúster de tres nodos sin recursos para evacuar la réplica o el testigo manteniendo una protección completa. Otro ejemplo consiste en un clúster de cuatro nodos con objetos RAID-5 ya implementados. En el último caso, no habrá espacio para mover parte de la fracción RAID-5, ya que los objetos RAID-5 requieren un mínimo de cuatro nodos.

Aún así, se podrán habilitar la desduplicación y la compresión, y usar la opción Permitir redundancia reducida. Esta opción mantiene las máquinas virtuales en ejecución, pero puede que estas no sean capaces de tolerar el nivel total de errores definidos en la directiva de almacenamiento de máquina virtual. Por tanto, durante el cambio de formato para la desduplicación y la compresión, existiría el riesgo temporal de que las máquinas virtuales perdiesen datos. vSAN restaura la redundancia y el cumplimiento completos una vez finalizada la conversión de formato.

Agregar o quitar discos con desduplicación y compresión habilitadas

Cuando se agregan discos a un clúster de vSAN donde se han habilitado la desduplicación y la compresión, se aplican unas consideraciones específicas.

- Puede agregar un disco de capacidad a un grupo de discos con la desduplicación y la compresión habilitadas. No obstante, para una desduplicación y compresión más eficientes, en vez de agregar discos de capacidad, cree un grupo de discos para aumentar la capacidad de almacenamiento del clúster.
- Cuando se quita un discos de un nivel de memoria caché, se quita el grupo de discos completo. Si se quita un disco de nivel de memoria caché cuando la desduplicación y la compresión están habilitadas, se activa la evacuación de datos.
- La desduplicación y la compresión se implementan a nivel de grupo de discos. No puede quitar un disco de capacidad del clúster con la desduplicación y la compresión habilitadas. Deberá eliminar el grupo de discos completo.
- Si se produce un error en un disco de capacidad, no se podrá acceder a ninguno de los discos del grupo. Para solucionar este problema, identifique y sustituya el componente con errores inmediatamente. Al quitar el grupo de discos, use la opción Sin migración de datos.

Usar la codificación de borrado RAID 5 o RAID 6

Puede utilizar la codificación de borrado RAID 5 o RAID 6 para ofrecer una protección frente a la pérdida de datos y aumentar la eficiencia del almacenamiento. La codificación de borrado puede proporcionar el mismo nivel de protección de datos que el reflejo (RAID 1) y, al mismo tiempo, usar menos capacidad de almacenamiento.

La codificación de borrado RAID 5 o RAID 6 permite que vSAN tolere los errores de hasta dos dispositivos de capacidad del almacén de datos. Puede configurar RAID 5 en clústeres basados íntegramente en tecnología flash con cuatro o más dominios de errores. Puede configurar RAID 5 o RAID 6 en clústeres basados íntegramente en tecnología flash con seis o más dominios de errores.

La codificación de borrado RAID 5 o RAID 6 requiere menos capacidad adicional para proteger los datos en comparación con el reflejo RAID 1. Por ejemplo, una máquina virtual protegida con un valor de **Primary level of failures to tolerate** (Nivel principal de errores que se toleran) de 1 con RAID 1 requiere el doble del tamaño de disco virtual. Sin embargo, con RAID 5, se requiere 1,33 veces el tamaño de disco virtual. La siguiente tabla muestra una comparación general entre RAID 1 y RAID 5 o RAID 6.

Tabla 7-1. Capacidad requerida para almacenar y proteger los datos con diferentes niveles de RAID

Configuración de RAID	Nivel principal de errores que se toleran	Tamaño de los datos	Capacidad requerida
RAID 1 (reflejo)	1	100 GB	200 GB
RAID 5 o RAID 6 (codificación de borrado) con cuatro dominios de errores	1	100 GB	133 GB
RAID 1 (reflejo)	2	100 GB	300 GB
RAID 5 o RAID 6 (codificación de borrado) con seis dominios de errores	2	100 GB	150 GB

La codificación de borrado RAID 5 o RAID 6 es un atributo de directiva que puede aplicar a los componentes de las máquinas virtuales. Para utilizar RAID 5, establezca **Failure tolerance method** (Método de tolerancia ante errores) en **RAID-5/6 (Erasure Coding) - Capacity** (RAID-5/6 [codificación de borrado]: capacidad) y **Primary level of failures to tolerate** (Nivel principal de errores que se toleran) en 1. Para utilizar RAID 6, establezca **Failure tolerance method** (Método de tolerancia ante errores) en **RAID-5/6 (Erasure Coding) - Capacity** (RAID-5/6 [codificación de borrado]: capacidad) y **Primary level of failures to tolerate** (Nivel principal de errores que se toleran) en 2. La codificación de borrado RAID 5 o RAID 6 no admite un valor de 3 de **Primary level of failures to tolerate** (Nivel principal de errores que se toleran).

Para utilizar RAID 1, establezca **Failure tolerance method** (Método de tolerancia ante errores) en **RAID-1 (Mirroring) - Performance** (RAID-1 [reflejo]: rendimiento). El reflejo RAID 1 requiere menos operaciones de E/S en los dispositivos de almacenamiento y, por lo tanto, puede proporcionar un mejor rendimiento. Por ejemplo, una resincronización del clúster demora menos tiempo en completarse con RAID 1.

Para obtener más información sobre la configuración de las directivas, consulte Capítulo 12, "Usar las directivas de vSAN," página 135.

Consideraciones de diseño de RAID 5 o RAID 6

Considere estas directrices al configurar la codificación de borrado RAID 5 o RAID 6 en un clúster de vSAN.

- La codificación de borrado RAID 5 o RAID 6 está disponible solo en grupos de discos basados íntegramente en tecnología flash.
- Se requiere el formato en disco versión 3.0 o posterior para admitir RAID 5 o RAID 6.
- Deberá tener una licencia válida para poder habilitar RAID 5/6 en un clúster.
- RAID 5/6 no se admite en los clústeres ampliados.
- Puede lograr ahorros de espacio adicionales al habilitar la desduplicación y la compresión en el clúster de vSAN.

Usar cifrado en un clúster de vSAN

8

Es posible utilizar el cifrado de datos en reposo para proteger los datos en el clúster de vSAN.

vSAN puede realizar cifrado de datos en reposo. Los datos se cifran después de que se llevan a cabo todas las otras operaciones de procesamiento, como la desduplicación. El cifrado de datos en reposo protege los datos de los dispositivos de almacenamiento, en caso de que un dispositivo se quite del clúster.

Para utilizar el cifrado en el clúster de vSAN, se requiere algo de preparación. Una vez que el entorno está configurado, se puede habilitar el cifrado en el clúster de vSAN.

El cifrado de vSAN requiere un servidor de administración de claves (Key Management Server, KMS) externo, el sistema vCenter Server y los hosts ESXi. vCenter Server solicita claves de cifrado desde un KMS externo. El KMS genera y almacena las claves, y vCenter Server obtiene los identificadores de claves del KMS y los distribuye en los hosts ESXi.

vCenter Server no almacena las claves del KMS, pero sí conserva una lista de identificadores de claves.

Este capítulo cubre los siguientes temas:

Cómo funciona el cifrado de vSAN

Cuando se habilita el cifrado, vSAN cifra todo el contenido del almacén de datos de vSAN. Como se cifra la totalidad de los archivos, todas las máquinas virtuales y sus correspondientes datos quedan protegidos. Solo los administradores con privilegios de cifrado pueden realizar tareas de cifrado y descifrado.

vSAN utiliza las claves de cifrado de la siguiente manera:

- vCenter Server solicita a KMS una clave de cifrado de claves (Key Encryption Key, KEK) AES-256. vCenter Server almacena solo el identificador de la KEK, pero no la clave en sí.
- El host ESXi cifra los datos del disco mediante el modo AES-256 XTS estándar del sector. Cada disco tiene una clave de cifrado de datos (Data Encryption Key, DEK) diferente que se genera al azar.
- Cada host ESXi usa la KEK para cifrar sus DEK y almacena las DEK cifradas en el disco. El host no almacena la KEK en el disco. Si un host se reinicia, solicita a KMS la KEK con el identificador correspondiente. A continuación, el host puede descifrar sus DEK según lo necesite.

- La clave de un host no se usa para cifrar datos, sino volcados de núcleos. Todos los hosts de un mismo clúster usan la misma clave de host. Al recopilar paquetes de soporte, se genera una clave al azar para volver a cifrar los volcados de núcleo. Use una contraseña al cifrar la clave al azar.

Cuando un host se reinicia, no monta sus grupos de discos hasta recibir la KEK. Este proceso puede tardar varios minutos o más en completarse. Es posible supervisar el estado de los grupos de discos en vSAN Health Service, en **Discos físicos > Estado de software**.

Consideraciones de diseño para el cifrado de vSAN

Tenga en cuenta las siguientes directrices al trabajar con el cifrado de vSAN.

- No implemente el servidor KMS en el mismo almacén de datos de vSAN que planea cifrar.
- El cifrado requiere gran consumo de CPU. AES-NI mejora ampliamente el rendimiento de cifrado. Habilite AES-NI en el BIOS.
- El host testigo de un clúster ampliado no participa en el cifrado de vSAN. Solo se almacenan metadatos en el host testigo.
- Establezca una directiva para los volcados de núcleo. Los volcados de núcleo se cifran debido a que pueden contener información confidencial como claves. Al descifrar un volcado de núcleo, maneje la información confidencial con cuidado. Los volcados de núcleo de ESXi pueden contener claves para el host ESXi y para los datos que este contiene.
  - Siempre utilice una contraseña para recopilar un paquete de `vm-support`. Puede especificar la contraseña al generar el paquete de soporte desde vSphere Web Client o puede utilizar el comando `vm-support`.

    La contraseña vuelve a cifrar los volcados de núcleo que utilizan claves internas de manera que estos volcados empleen claves basadas en la contraseña. Posteriormente, se puede usar la contraseña para descifrar cualquier volcado de núcleo cifrado que pudiera estar incluido en el paquete de soporte. Esto no afecta a los volcados de núcleo ni a los registros sin cifrar.
  - La contraseña que especificó durante la creación del paquete de `vm-support` no persiste en los componentes de vSphere. Es su responsabilidad llevar un registro de las contraseñas de los paquetes de soporte.

Configurar el clúster de KMS

Un clúster de servidor de administración de claves (Key Management Server, KMS) proporciona las claves que pueden usarse para cifrar el almacén de datos de vSAN.

Para poder cifrar el almacén de datos de vSAN, se debe configurar un clúster de KMS a fin de admitir el cifrado. Esa tarea incluye agregar el KMS a vCenter Server y establecer confianza con el KMS. vCenter Server proporciona claves de cifrado desde el clúster de KMS.

KMS debe ser compatible con el protocolo estándar de interoperabilidad de administración de claves (KMIP) 1.1.

Agregar un KMS a vCenter Server

Los servidores de administración de claves (KMS) se agregan a los sistemas vCenter Server desde vSphere Web Client.

vCenter Server crea un clúster de KMS cuando se agrega la primera instancia de KMS. Si configura el clúster de KMS en dos o más instancias de vCenter Server, asegúrese de usar el mismo nombre de clúster de KMS.

NOTA: No implemente los servidores KMS en el clúster de vSAN que planea cifrar. Si se produce un error, los hosts del clúster de vSAN deberán comunicarse con el servidor KMS.

- Al agregar un servidor KMS, se solicita establecer este clúster como predeterminado. Más adelante, es posible cambiar explícitamente el clúster predeterminado.
- Después de que vCenter Server cree el primer clúster, es posible agregar instancias de KMS del mismo proveedor al clúster.
- Se puede configurar el clúster con una sola instancia de KMS.
- Si el entorno admite soluciones de KMS de diferentes proveedores, es posible agregar varios clústeres de KMS.

Prerequisitos

- Compruebe que el servidor de claves se encuentre en *Matrices de compatibilidad de vSphere* y que cumpla con KMIP 1.1.
- Compruebe que dispone de los privilegios necesarios: **Cryptographer.ManageKeyServers (Criptógrafo.AdministrarServidoresClaves).**
- No se admite la conexión con un KMS exclusivamente por medio de una dirección IPv6.
- No se admite la conexión con un KMS a través de un servidor proxy que requiera nombre de usuario o contraseña.

Procedimiento

1 Inicie sesión en el sistema vCenter Server mediante vSphere Web Client.

2 Examine la lista de inventario y seleccione la instancia de vCenter Server.

3 Haga clic en **Configure** (Configurar) y en **Key Management Servers** (Servidores de administración de claves).

4 Haga clic en **Add KMS** (Agregar KMS), especifique la información de KMS en el asistente y haga clic en **OK** (Aceptar).

Opción	Valor
KMS cluster (Clúster de KMS)	Seleccione **Create new cluster** (Crear nuevo clúster) para crear un nuevo clúster. Si existe un clúster, puede seleccionarlo.
Cluster name (Nombre de clúster)	Nombre del clúster de KMS. Puede utilizar este nombre para conectarse al KMS si la instancia de vCenter Server deja de estar disponible.
Server alias (Alias de servidor)	Alias del KMS. Puede utilizar este alias para conectarse al KMS si la instancia de vCenter Server deja de estar disponible.
Server address (Dirección de servidor)	Dirección IP o FQDN del KMS.
Server port (Puerto de servidor)	Puerto en el cual vCenter Server se conecta al KMS.
Proxy address (Dirección de proxy)	Dirección de proxy opcional para conectarse al KMS.
Proxy port (Puerto de proxy)	Puerto de proxy opcional para conectarse al KMS.

Opción	Valor
User name (Nombre de usuario)	Algunos proveedores de KMS permiten a los usuarios especificar un nombre de usuario y una contraseña para aislar las claves de cifrado utilizadas por distintos usuarios o grupos. Especifique un nombre de usuario solo si el KMS admite esta funcionalidad y si piensa utilizarla.
Password (Contraseña)	Algunos proveedores de KMS permiten a los usuarios especificar un nombre de usuario y una contraseña para aislar las claves de cifrado utilizadas por distintos usuarios o grupos. Especifique una contraseña solo si el KMS admite esta funcionalidad y si piensa utilizarla.

Establecer una conexión de confianza mediante el intercambio de certificados

Después de agregar el KMS al sistema de vCenter Server, puede establecer una conexión de confianza. El proceso exacto depende de los certificados que el KMS acepte y de la directiva de la empresa.

Prerequisitos

Agregue el clúster KMS.

Procedimiento

1 Inicie sesión en vSphere Web Client y seleccione un sistema vCenter Server.

2 Haga clic en **Configurar** y seleccione **Servidores de administración de claves**.

3 Seleccione la instancia de KMS con la cual desea establecer una conexión de confianza.

4 Haga clic en **Establecer confianza con KMS**.

5 Seleccione la opción adecuada para el servidor y complete los pasos.

Opción	Consulte
Certificado de CA raíz	"Usar la opción Certificado de CA raíz para establecer una conexión de confianza," página 86.
Certificado	"Usar la opción Certificado para establecer una conexión de confianza," página 87.
Nueva solicitud de firma de certificado	"Usar la opción New Certificate Signing Request (Nueva solicitud de firma del certificado) para establecer una conexión de confianza," página 87.
Cargar certificado y clave privada	"Usar la opción Cargar certificado y clave privada para establecer una conexión de confianza," página 88.

Usar la opción Certificado de CA raíz para establecer una conexión de confianza

Algunos proveedores de KMS, como SafeNet, requieren que se cargue un certificado de CA raíz al KMS. Este KMS establece una conexión de confianza con todos los certificados firmados por la entidad de certificación de raíz.

El certificado de CA raíz que utiliza el cifrado de máquinas virtuales de vSphere es un certificado autofirmado que se almacena en un almacén separado en VMware Endpoint Certificate Store (VECS) en el sistema de vCenter Server.

NOTA: Genere un certificado de CA raíz solo si desea reemplazar los certificados existentes. En ese caso, los demás certificados que están firmados por esa entidad de certificación raíz dejan de ser válidos. Se puede generar un nuevo certificado de CA raíz como parte de este flujo de trabajo.

Procedimiento

1 Inicie sesión en vSphere Web Client y seleccione un sistema vCenter Server.

2 Haga clic en **Configurar** y seleccione **Servidores de administración de claves**.

3 Seleccione la instancia de KMS con la cual desea establecer una conexión de confianza.

4 Seleccione **Certificado de CA raíz** y haga clic en **Aceptar**.

El cuadro de diálogo Descargar certificado de CA raíz se rellena con el certificado raíz que vCenter Server utiliza para el cifrado. Este certificado se almacena en el almacén VECS.

5 Copie el certificado en el portapapeles o descárguelo como un archivo.

6 Siga las instrucciones de su proveedor de KMS para cargar el certificado al sistema.

NOTA: Algunos proveedores de KMS, por ejemplo SafeNet, requieren que el proveedor de KMS reinicie el KMS para seleccionar el certificado raíz que se cargó.

Qué hacer a continuación

Finalice el intercambio de certificados. Consulte "Completar la instalación de confianza," página 89.

Usar la opción Certificado para establecer una conexión de confianza

Algunos proveedores de KMS, como Vormetric, requieren que se cargue el certificado de vCenter Server al KMS. Después de la carga, el KMS acepta el tráfico proveniente de un sistema con ese certificado.

vCenter Server genera un certificado para proteger las conexiones con el KMS. El certificado se almacena en un almacén de claves separado en VMware Endpoint Certificate Store (VECS) en el sistema de vCenter Server.

Procedimiento

1 Inicie sesión en vSphere Web Client y seleccione un sistema vCenter Server.

2 Haga clic en **Configurar** y seleccione **Servidores de administración de claves**.

3 Seleccione la instancia de KMS con la cual desea establecer una conexión de confianza.

4 Seleccione **Certificate** (Certificado) y haga clic en **OK** (Aceptar).

El cuadro de diálogo Download Certificate (Descargar certificado) se rellena con el certificado raíz que vCenter Server utiliza para el cifrado. Este certificado se almacena en el almacén VECS.

NOTA: No genere un certificado nuevo a menos que desee reemplazar los certificados existentes.

5 Copie el certificado en el portapapeles o descárguelo como un archivo.

6 Siga las instrucciones de su proveedor de KMS para cargar el certificado al KMS.

Qué hacer a continuación

Finalice la relación de confianza. Consulte "Completar la instalación de confianza," página 89.

Usar la opción New Certificate Signing Request (Nueva solicitud de firma del certificado) para establecer una conexión de confianza

Algunos proveedores de KMS, por ejemplo Thales, requieren que vCenter Server genere una solicitud de firma del certificado (Certificate Signing Request, CSR) y que se envíe esa CSR al KMS. El KMS firma la CSR y devuelve el certificado firmado. El certificado firmado se puede cargar en vCenter Server.

El uso de la opción **New Certificate Signing Request** (Nueva solicitud de firma del certificado) es un proceso de dos pasos. Primero debe generar la CSR y enviarla al proveedor de KMS. A continuación, cargue el certificado firmado que recibió del proveedor de KMS a vCenter Server.

Procedimiento

1 Inicie sesión en vSphere Web Client y seleccione un sistema vCenter Server.

2 Haga clic en **Configurar** y seleccione **Servidores de administración de claves**.

3 Seleccione la instancia de KMS con la cual desea establecer una conexión de confianza.

4 Seleccione **New Certificate Signing Request** (Nueva solicitud de firma del certificado) y haga clic en **OK** (Aceptar).

5 En el cuadro de diálogo, copie el certificado completo del cuadro de texto en el portapapeles o descárguelo como un archivo, y haga clic en **OK** (Aceptar).

   Use el botón **Generate new CSR** (Generar nueva CSR) del cuadro de diálogo únicamente si desea generar una CSR de forma explícita. Al usar esa opción, todos los certificados firmados basados en la CSR anterior dejan de ser válidos.

6 Siga las instrucciones de su proveedor de KMS para enviar la CSR.

7 Cuando reciba el certificado firmado del proveedor de KMS, vuelva a hacer clic en **Key Management Servers** (Servidores de administración de claves) y vuelva a seleccionar **New Certificate Signing Request** (Nueva solicitud de firma del certificado).

8 Pegue el certificado firmado en el cuadro de texto inferior o haga clic en **Upload File** (Cargar archivo) y cargue el archivo; luego, haga clic en **OK** (Aceptar).

Qué hacer a continuación

Finalice la relación de confianza. Consulte "Completar la instalación de confianza," página 89.

Usar la opción Cargar certificado y clave privada para establecer una conexión de confianza

Algunos proveedores de KMS, como HyTrust, requieren que se cargue el certificado del servidor KMS y la clave privada al sistema de vCenter Server.

Algunos proveedores de KMS generan un certificado y una clave privada para la conexión y los vuelven disponibles para el usuario. Una vez que haya cargado los archivos, el KMS establecerá una conexión de confianza con su instancia de vCenter Server.

Prerequisitos

- Solicite un certificado y una clave privada al proveedor de KMS. Los archivos son archivos X509 en formato PEM.

Procedimiento

1 Inicie sesión en vSphere Web Client y seleccione un sistema vCenter Server.

2 Haga clic en **Configurar** y seleccione **Servidores de administración de claves**.

3 Seleccione la instancia de KMS con la cual desea establecer una conexión de confianza.

4 Seleccione **Cargar certificado y clave privada** y haga clic en **Aceptar**.

5 Pegue el certificado que recibió del proveedor de KMS en el cuadro de texto superior o haga clic en **Cargar certificado** para cargar el archivo del certificado.

6 Pegue el archivo de claves en el cuadro de texto inferior o haga clic en **Cargar archivo** para cargar el archivo de claves.

7 Haga clic en **Aceptar**.

Qué hacer a continuación

Finalice la relación de confianza. Consulte "Completar la instalación de confianza," página 89.

Establecer el clúster de KMS predeterminado

Si no establece el primer clúster como el clúster predeterminado o si el entorno usa varios clústeres y elimina el clúster predeterminado, debe establecer el clúster de KMS como predeterminado.

Prerequisitos

Como práctica recomendada, compruebe que el estado de conexión en la pestaña Servidores de administración de claves sea Normal y tenga una marca de verificación verde.

Procedimiento

1 Inicie sesión en vSphere Web Client y seleccione un sistema vCenter Server.

2 Haga clic en la pestaña **Configurar** y en **Servidores de administración de claves** en **Más**.

3 Seleccione el clúster y haga clic en **Establecer el clúster de KMS como predeterminado**.

   No seleccione el servidor. El menú para establecer el clúster como predeterminado está disponible para ese clúster solamente.

4 Haga clic en **Yes** (Sí).

   La palabra `default` aparece junto al nombre del clúster.

Completar la instalación de confianza

A menos que el cuadro de diálogo **Agregar servidor** le haya solicitado confiar en el KMS, debe establecer la confianza explícitamente una vez finalizado el intercambio de certificados.

Es posible completar la instalación de confianza, es decir, hacer que vCenter Server confíe en el KMS, ya sea confiando en el KMS o cargando un certificado de KMS. Tiene dos opciones:

- Confiar en el certificado explícitamente por medio de la opción **Actualizar certificado de KMS**.
- Cargar un certificado de hoja de KMS o el certificado de CA de KMS en vCenter Server por medio de la opción **Cargar certificado de KMS**.

NOTA: Si carga el certificado de CA raíz o el certificado de CA intermedia, vCenter Server confía en todos los certificados que firma esa CA. Si desea obtener una seguridad más solida, cargue un certificado de hoja o un certificado de CA intermedia que controle el proveedor de KMS.

Procedimiento

1 Inicie sesión en vSphere Web Client y seleccione un sistema vCenter Server.

2 Haga clic en **Configurar** y seleccione **Servidores de administración de claves**.

3 Seleccione la instancia de KMS con la cual desea establecer una conexión de confianza.

4 Para establecer la relación de confianza, actualice o cargue el certificado de KMS.

Opción	Acción
Actualizar certificado de KMS	a Haga clic en **Todas las acciones** y seleccione **Actualizar certificado de KMS**. b En el cuadro de diálogo que aparece, haga clic en **Confiar**.
Cargar certificado de KMS	a Haga clic en **Todas las acciones** y seleccione **Cargar certificado de KMS**. b En el cuadro de diálogo que aparece, haga clic en **Cargar archivo**, cargue un archivo de certificado y haga clic en **Aceptar**.

Habilitar el cifrado en un nuevo clúster de vSAN

Puede habilitar el cifrado cuando se configura un nuevo clúster de vSAN.

Prerequisitos

- Privilegios necesarios:
  - **Host.Inventory.EditCluster** (Host.Inventario.EditarClúster)
  - **Cryptographer.ManageEncryptionPolicy**(Criptógrafo.AdministrarDirectivaCifrado)
  - **Cryptographer.ManageKMS**(Criptógrafo.AdministrarKMS)
  - **Cryptographer.ManageKeys**(Criptógrafo.AdministrarClaves)
- Se debe haber configurado un clúster de KMS y establecido una conexión de confianza entre vCenter Server y KMS.

Procedimiento

1. Desplácese hasta un clúster existente en vSphere Web Client.
2. Haga clic en la pestaña **Configurar**.
3. En vSAN, seleccione **General** y haga clic en el botón **Configure vSAN** (Configurar vSAN).
4. En la página **vSAN capabilites** (Funcionalidades de vSAN), marque la casilla **Encryption** (Cifrado) y seleccione un clúster de KMS.

   NOTA: Asegúrese de que no esté marcada la casilla **Erase disks before use** (Borrar discos antes del uso), a menos que desee borrar los datos actuales de los dispositivos de almacenamiento durante el cifrado.

5. En la página **Reclamar discos**, especifique los discos que se reclamarán para el clúster de vSAN.
   a. Seleccione el dispositivo flash que se utilizará para capacidad y haga clic en el icono **Claim for capacity tier** (Recuperar para nivel de capacidad) ().
   b. Seleccione un dispositivo flash que se utilizará para almacenamiento en caché y haga clic en el icono **Claim for cache tier** (Recuperar para nivel de almacenamiento en caché) ().
6. Complete la configuración del clúster.

En el clúster de vSAN, se habilita el cifrado de datos en reposo. vSAN cifra todos los datos que se agregan al almacén de datos de vSAN.

Generar nuevas claves de cifrado

Es posible crear nuevas claves de cifrado en caso de que una clave caduque o se vea comprometida.

Al generar nuevas claves de cifrado para el clúster de vSAN, están disponibles las siguientes opciones:

- Si genera una nueva KEK, todos los hosts del clúster de vSAN reciben la nueva KEK del KMS. La DEK de cada host se vuelve a cifrar con la nueva KEK.
- Si elige volver a cifrar todos los datos con claves nuevas, se generan una nueva KEK y una nueva DEK. Para volver a cifrar los datos, es preciso reformatear el disco en forma sucesiva.

Prerequisitos

- Privilegios necesarios:
  - **Host.Inventory.EditCluster** (Host.Inventario.EditarClúster)
  - **Cryptographer.ManageKeys**(Criptógrafo.AdministrarClaves)
- Se debe haber configurado un clúster de KMS y establecido una conexión de confianza entre vCenter Server y KMS.

Procedimiento

1. Desplácese hasta el clúster del host de vSAN en vSphere Web Client.
2. Haga clic en la pestaña **Configurar**.
3. En vSAN, seleccione **General**.
4. En el panel vSAN está activado, haga clic en el botón **Generar nuevas claves de cifrado**.
5. Para generar una nueva KEK, haga clic en **OK** (Aceptar). Las DEK se volverán a cifrar con la nueva KEK.
   - Para generar una nueva KEK y nuevas DEK, y para volver a cifrar todos los datos del clúster de vSAN, active la siguiente casilla: **También vuelva a cifrar todos los datos en el almacenamiento con nuevas claves**.
   - Si el clúster de vSAN tiene recursos limitados, marque la casilla **Permitir redundancia reducida**. Si permite la redundancia reducida, es posible que los datos estén en riesgo durante la operación de reformateo de disco.

Habilitar el cifrado de vSAN en un clúster de vSAN existente

Puede habilitar el cifrado mediante la edición de los parámetros de configuración de un clúster de vSAN existente.

Prerequisitos

- Privilegios necesarios:
  - **Host.Inventory.EditCluster** (Host.Inventario.EditarClúster)
  - **Cryptographer.ManageEncryptionPolicy**(Criptógrafo.AdministrarDirectivaCifrado)
  - **Cryptographer.ManageKMS**(Criptógrafo.AdministrarKMS)
  - **Cryptographer.ManageKeys**(Criptógrafo.AdministrarClaves)
- Se debe haber configurado un clúster de KMS y establecido una conexión de confianza entre vCenter Server y KMS.
- El reclamo de discos del clúster debe estar configurado en modo manual.

Procedimiento

1. Desplácese hasta el clúster del host de vSAN en vSphere Web Client.
2. Haga clic en la pestaña **Configurar**.
3. En vSAN, seleccione **General**.
4. En el panel vSAN está activado, haga clic en el botón **Editar**.
5. En el cuadro de diálogo Editar configuración de vSAN, active la casilla **Cifrado** y seleccione un clúster de KMS.

6 (Opcional) Si los dispositivos de almacenamiento del clúster contienen datos confidenciales, marque la casilla **Erase disks before use** (Borrar discos antes del uso).

   Con esta configuración, vSAN limpia los datos existentes de los dispositivos de almacenamiento durante el cifrado.

7 Haga clic en **OK** (Aceptar).

Se lleva a cabo un reformateo sucesivo de todos los grupos de discos mientras vSAN cifra todos los datos en el almacén de datos de vSAN.

Cifrado y volcados de núcleo en vSAN

Si el clúster de vSAN utiliza cifrado y si se produce un error en el host ESXi, el volcado de núcleo resultante se cifra para proteger los datos del cliente. Los volcados de núcleo que se incluyen en el paquete de `vm-support` también están cifrados.

NOTA: Los volcados de núcleo pueden contener información confidencial. Siga la directiva de seguridad de datos y privacidad de la organización al gestionar el volcado de núcleo.

Volcados de núcleo en hosts ESXi

Cuando un host ESXi se bloquea, se genera un volcado de núcleo cifrado y el host se reinicia. El volcado de núcleo se cifra con la clave de host que se encuentra en la memoria caché de claves de ESXi. Lo que puede hacer a continuación depende de diversos factores.

- En la mayoría de los casos, vCenter Server recupera la clave del host del KMS e intenta insertar la clave en el host ESXi después de reiniciar. Si la operación se realiza correctamente, se puede generar el paquete de `vm-support` y descifrar o volver a cifrar el volcado de núcleo.
- Si vCenter Server no puede conectarse al host ESXi, tal vez se pueda recuperar la clave del KMS.
- Si el host usó una clave personalizada que no es igual a la clave que vCenter Server inserta en el host, no se podrá manipular el volcado de núcleo. Evite usar claves personalizadas.

Volcados de núcleo y paquetes de vm-support

Si se comunica con el soporte técnico de VMware debido a un error grave, el representante de soporte, por lo general, le pedirá que genere un paquete de `vm-support`. El paquete incluye archivos de registro y otra información, incluso volcados de núcleo. Si los representantes de soporte no pueden resolver los inconvenientes al analizar los archivos de registro y otra información, el usuario puede descifrar los volcados de núcleo para habilitar la información relevante. Siga la directiva de seguridad y privacidad de la organización para proteger la información confidencial, como las claves de host.

Volcados de núcleo de sistemas vCenter Server

Un volcado de núcleo de un sistema vCenter Server no está cifrado. vCenter Server ya contiene información posiblemente confidencial. Como mínimo, asegúrese de que el sistema Windows donde se ejecuta vCenter Server Appliance o que vCenter Server estén protegidos. Asimismo, también se recomienda apagar los volcados de núcleo del sistema de vCenter Server. Otra información de los archivos de registro puede ayudar a determinar el problema.

Recopilar un paquete de vm-support para un host de ESXi en un clúster de vSAN cifrado

Cuando se habilita el cifrado en un clúster de vSAN, se cifran todos los volcados de núcleo en el paquete de `vm-support`. Es posible recopilar el paquete desde vSphere Web Client y especificar una contraseña si se planea descifrar el volcado de núcleo más adelante.

El paquete de `vm-support` incluye archivos de registro y archivos de volcado de núcleo, entre otros.

Prerequisitos

Notifique a su representante de soporte que se habilitó el cifrado para el clúster de vSAN. Es posible que el representante le pida descifrar los volcados de núcleo para extraer información relevante.

NOTA: Los volcados de núcleo pueden contener información confidencial. Siga la directiva de seguridad y privacidad de la organización para proteger la información confidencial, como las claves de host.

Procedimiento

1 Inicie sesión en vCenter Server con vSphere Web Client.

2 Haga clic en **Hosts and Clusters** (Hosts y clústeres) y, a continuación, haga clic con el botón derecho en el host ESXi.

3 Seleccione **Export System Logs** (Exportar registros del sistema).

4 En el cuadro de diálogo, seleccione **Password for encrypted core dumps** (Contraseña para volcados de núcleo cifrados) y, a continuación, especifique y confirme una contraseña.

5 Deje los valores predeterminados para las otras opciones o realice cambios si así lo requiere el soporte técnico de VMware, y haga clic en **Finish** (Finalizar).

6 Especifique una ubicación para el archivo.

7 Si su representante de soporte le pidió descifrar el volcado de núcleo en el paquete de `vm-support`, inicie sesión en cualquier host ESXi y siga estos pasos.

   a Inicie sesión en ESXi y conéctese al directorio donde se encuentra el paquete de `vm-support`.

   El nombre de archivo sigue el patrón **`esx.fecha_y_hora.tgz`**.

   b Asegúrese de que el directorio tenga suficiente espacio para el paquete, el paquete descomprimido y el paquete nuevamente comprimido, o mueva el paquete.

   c Extraiga el paquete en el directorio local.

   ```
   vm-support -x *.tgz .
   ```

   La jerarquía de archivos resultante puede contener los archivos de volcado de núcleo para el host ESXi, generalmente en `/var/core`, y puede contener varios archivos de volcado de núcleo de las máquinas virtuales.

   d Descifre cada archivo de volcado de núcleo cifrado por separado.

   ```
   crypto-util envelope extract --offset 4096 --keyfile vm-support-incident-key-file
   --password encryptedZdump decryptedZdump
   ```

   vm-support-incident-key-file es el archivo de claves de incidentes que se encuentra en el nivel superior del directorio.

   encryptedZdump es el nombre del archivo de volcado de núcleo cifrado.

   decryptedZdump es el nombre del archivo que genera el comando. Procure que el nombre sea similar al nombre de *encryptedZdump*.

e Proporcione la contraseña que especificó al crear el paquete de `vm-support`.

f Elimine los volcados de núcleo cifrados y vuelva a comprimir el paquete.

```
vm-support --reconstruct
```

8 Elimine los archivos que contengan información confidencial.

Descifrar o volver a cifrar un volcado de núcleo cifrado

Para descifrar o volver a cifrar un volcado de núcleo cifrado en el host ESXi, se puede usar la CLI `crypto-util`.

Puede descifrar y examinar por su cuenta los volcados de núcleo en el paquete de `vm-support`. Los volcados de núcleo pueden contener información confidencial. Siga la directiva de seguridad y privacidad de la organización para proteger la información confidencial, como las claves de host.

Para obtener detalles sobre la forma de volver a cifrar un volcado de núcleo y usar otras funciones de `crypto-util`, consulte la ayuda de la línea de comandos.

NOTA: `crypto-util` es para usuarios avanzados.

Prerequisitos

La clave de host ESXi que se usó para cifrar el volcado de núcleo debe estar disponible en el host ESXi que generó el volcado de núcleo.

Procedimiento

1 Inicie sesión directamente en el host ESXi donde se produjo el volcado de núcleo.

Si el host ESXi se encuentra en el modo de bloqueo, o si el acceso SSH está deshabilitado, es posible que deba habilitar el acceso primero.

2 Determine si el volcado de núcleo está cifrado.

Opción	Descripción
Supervisar el volcado de núcleo	`crypto-util envelope describe vmmcores.ve`
archivo zdump	`crypto-util envelope describe --offset 4096` *zdumpFile*

3 Descifre el volcado de núcleo según su tipo.

Opción	Descripción
Supervisar el volcado de núcleo	`crypto-util envelope extract vmmcores.ve vmmcores`
archivo zdump	`crypto-util envelope extract --offset 4096` *zdumpEncrypted zdumpUnencrypted*

Actualizar el clúster de vSAN 9

La actualización de vSAN es un proceso de varias etapas, en el cual los procedimientos de actualización se deben llevar a cabo en el orden que se describe aquí.

Antes de intentar realizar la actualización, asegúrese de comprender claramente todo el proceso de actualización, a fin de garantizar una actualización correcta y sin interrupciones. Si no está familiarizado con el procedimiento general de actualización de vSphere, primero debe consultar el documento *Actualización de vSphere*.

NOTA: Si no se respeta la secuencia de tareas para la actualización que se describe aquí, se perderán datos y se producirán errores en el clúster.

La actualización del clúster de vSAN se lleva a cabo en la siguiente secuencia de tareas.

1 Actualización de vCenter Server. Consulte la documentación sobre la *actualización de vSphere*.

2 Actualización de los hosts ESXi hosts. Consulte "Actualizar los hosts ESXi," página 98. Para obtener información sobre la migración y la preparación para la actualización de los hosts ESXi, consulte el documento *Actualización de vSphere*.

3 Actualice el formato de disco de vSAN. La actualización del formato de disco es opcional, pero, para obtener los mejores resultados, actualice los objetos a la versión más reciente. El formato en disco expone el entorno al conjunto completo de características de vSAN. Consulte "Actualizar el formato de disco de vSAN mediante RVC," página 103.

Este capítulo cubre los siguientes temas:

Antes de actualizar vSAN

Planifique y diseñe la actualización para que sea a prueba de errores. Antes de intentar actualizar vSAN, compruebe que el entorno cumpla con los requisitos de hardware y software de vSphere.

Requisito previo de actualización

Tenga en cuenta los aspectos que pueden retrasar el proceso general de actualización. Para obtener instrucciones y prácticas recomendadas, consulte el documento *Actualización de vSphere*.

Consulte los requisitos clave antes de actualizar el clúster a vSAN 6.6.

Tabla 9-1. Requisito previo de actualización

Requisitos previos de actualización	Descripción
Software, hardware, controladores, firmware y controladoras de E/S de almacenamiento	Compruebe que los componentes de software y hardware, los controladores, el firmware y las controladoras de E/S de almacenamiento que tiene pensado usar sean compatibles con vSAN 6.6 y versiones posteriores, y que aparezcan en el sitio web de la guía de compatibilidad de VMware, a la cual puede acceder mediante la siguiente URL: http://www.vmware.com/resources/compatibility/search.php.
Versión de vSAN	Compruebe que esté usando la versión más reciente de vSAN. Si actualmente ejecuta una versión beta y tiene pensado actualizar a vSAN 6.6, se producirá un error en la actualización. Cuando se actualiza desde una versión beta, se debe realizar una implementación nueva de vSAN.
Espacio en disco	Compruebe que tenga espacio suficiente disponible para completar la actualización de la versión de software. La cantidad de almacenamiento en disco que se necesita para la instalación de vCenter Server depende de la configuración de vCenter Server. Para obtener instrucciones sobre el espacio en disco que se necesita para la actualización de vSphere, consulte el documento *Actualización de vSphere* .
Formato de disco de vSAN	Asegúrese de contar con capacidad de almacenamiento suficiente para actualizar el formato de disco. Si la cantidad de espacio que libera no iguala la capacidad consumida del grupo de discos más grande, con el espacio disponible en los grupos de discos que no son los grupos de discos que se están convirtiendo, debe seleccionar **Allow reduced redundancy** (Permitir redundancia reducida) como la opción de migración de datos. Por ejemplo, el grupo de discos más grande de un clúster tiene 10 TB de capacidad física, pero solamente se están usando 5 TB. Será necesaria una capacidad de reserva adicional de 5 TB en otra ubicación del clúster, excepto los grupos de discos que se van a migrar. Al actualizar el formato de disco de vSAN, compruebe que los hosts no estén en modo de mantenimiento. Cuando cualquier host miembro de un clúster de vSAN entra en modo de mantenimiento, la capacidad del clúster se reduce de manera automática, ya que el host miembro deja de aportar almacenamiento al clúster y su capacidad deja de estar disponible para los datos. Para obtener información sobre los diversos modos de evacuación, consulte “Poner un miembro de un clúster de vSAN en modo de mantenimiento,” página 124.

Tabla 9‑1. Requisito previo de actualización (Continua)

Requisitos previos de actualización	Descripción
Hosts de vSAN	Asegúrese de haber puesto los hosts de vSAN en modo de mantenimiento y de haber seleccionado la opción **Garantizar accesibilidad a los datos** o **Evacuar todos los datos**. **Puede usar vSphere Update Manager para automatizar y probar el proceso de actualización.**Sin embargo, cuando se usa vSphere Update Manager para actualizar vSAN, el modo de evacuación predeterminado es **Garantizar accesibilidad a los datos**. Cuando se usa el modo **Garantizar accesibilidad a los datos**, los datos no quedan completamente protegidos y, si se produce un error durante la actualización de vSAN, es posible que se produzca una pérdida de datos inesperada. No obstante, el modo **Ensure data accessibility** (Garantizar accesibilidad a los datos) es más rápido que el modo **Evacuate all data** (Evacuar todos los datos), ya que no es necesario transferir todos los datos a otro host del clúster. Para obtener información sobre los diversos modos de evacuación, consulte "Poner un miembro de un clúster de vSAN en modo de mantenimiento," página 124.
Virtual Machines (Máquinas virtuales)	Compruebe que se haya creado una copia de seguridad de las máquinas virtuales.

Recomendaciones

Tenga en cuenta las siguientes recomendaciones al implementar hosts ESXi para su uso con vSAN:

- Si los hosts de ESXi están configurados con una capacidad de memoria de 512 GB o menos, use dispositivos SATADOM, SD, USB o discos duros como medios de instalación.
- Si los hosts de ESXi están configurados con una capacidad de memoria superior a 512 GB, use un dispositivo flash o un disco magnético independiente como dispositivo de instalación. Si usa un dispositivo independiente, compruebe que vSAN no reclama el dispositivo.
- Al arrancar un host vSAN desde un dispositivo SATADOM, debe usar un dispositivo de celdas de un solo nivel (single-level cell, SLC) y el tamaño del dispositivo de arranque debe ser de 16 GB como mínimo.

vSAN 6.5 y las versiones posteriores permiten ajustar los requisitos de tamaño de arranque para un host ESXi en un clúster de vSAN. Para obtener más información, consulte el artículo de la base de conocimientos de VMware en http://kb.vmware.com/kb/2147881.

Actualizar el host testigo en un clúster ampliado o de dos hosts

El host testigo de un clúster de dos hosts o un clúster ampliado se encuentra fuera del clúster de vSAN, pero se administra con la misma instancia de vCenter Server. Es posible usar el mismo proceso para actualizar el host testigo que se usa para un host de datos de vSAN.

No actualice el host testigo hasta que todos los hosts de datos se hayan actualizado y hayan salido del modo de mantenimiento.

El uso de vSphere Update Manager para actualizar hosts en paralelo puede provocar que el host testigo se actualice en paralelo con uno de los hosts de datos. Para evitar problemas de actualización, configure vSphere Update Manager de modo que no actualice el host testigo en paralelo con los hosts de datos.

Actualizar vCenter Server

La primera tarea que se realizará durante la actualización de vSAN es una actualización general de vSphere, que incluye la actualización de vCenter Server y los hosts ESXi.

VMware admite actualizaciones locales en sistemas de 64 bits de vCenter Server 4.x, vCenter Server 5.0.x, vCenter Server 5.1.x y vCenter Server 5.5 a vCenter Server 6.0 y posteriores. La actualización de vCenter Server incluye una actualización del esquema de la base de datos y una actualización de vCenter Server. En lugar de realizar una actualización local a vCenter Server, se puede utilizar otro equipo para llevar a cabo la actualización. Para obtener instrucciones detalladas y varias opciones de actualización, consulte el documento *Actualización de vSphere*.

Actualizar los hosts ESXi

Después de actualizar vCenter Server, la siguiente tarea en la actualización del clúster de vSAN es actualizar los hosts ESXi para que usen la versión actual.

Si tiene varios hosts en el clúster de vSAN y usa vSphere Update Manager para actualizarlos, el modo de evacuación predeterminado es **Garantizar accesibilidad a los datos**. Si usa este modo y se produce un error durante la actualización de vSAN, los datos quedarán expuestos a riesgos. Para obtener información sobre cómo trabajar con los modos de evacuación, consulte "Poner un miembro de un clúster de vSAN en modo de mantenimiento," página 124

Para obtener información sobre el uso de vSphere Update Manager, consulte el sitio web de documentación en https://www.vmware.com/support/pubs/vum_pubs.html.

Antes de intentar realizar una actualización de los hosts ESXi, consulte las prácticas recomendadas que se describen en el documento *Actualización de vSphere*. VMware proporciona varias opciones de actualización de ESXi. Seleccione la opción de actualización que resulte más adecuada para el tipo de host que va a actualizar. Para obtener más información sobre las diversas opciones de actualización, consulte el documento *Actualización de vSphere*.

Prerequisitos

- Compruebe que tenga espacio suficiente en disco para actualizar los hosts ESXi. Para obtener instrucciones en relación con los requisitos de espacio en disco, consulte el documento *Actualización de vSphere*.
- Compruebe que esté usando la versión más reciente de ESXi. Puede descargar la versión más reciente del instalador de ESXi desde el sitio web de descargas de productos VMware, en https://my.vmware.com/web/vmware/downloads.
- Compruebe que esté usando la versión más reciente de vCenter Server.
- Compruebe la compatibilidad de la configuración de red, la controladora de E/S de almacenamiento, el dispositivo de almacenamiento y el software de copia de seguridad.
- Compruebe que se haya creado una copia de seguridad de las máquinas virtuales.
- Use Distributed Resource Scheduler (DRS) para prevenir el tiempo de inactividad de las máquinas virtuales durante la actualización. Compruebe que el nivel de automatización de cada máquina virtual se configure en el modo **Fully Automated** (Completamente automatizado) para ayudar a DRS a migrar máquinas virtuales cuando los hosts entran en modo de mantenimiento. Como alternativa, también puede apagar todas las máquinas virtuales o ejecutar una migración manual.

Procedimiento

1 Coloque en modo de mantenimiento el host que desea actualizar.

Debe comenzar la ruta de acceso de actualización con los hosts ESXi 5.5 o los más recientes en el clúster de vSAN.

a Haga clic con el botón derecho en el host en el navegador de vSphere Web Client y seleccione **Maintenance Mode > Enter Maintenance Mode** (Modo de mantenimiento > Entrar en modo de mantenimiento).

b Seleccione el modo de evacuación **Ensure data accessibility** (Garantizar accesibilidad a los datos) o **Evacuate all data** (Evacuar todos los datos), según sus requisitos, y espere hasta que el host entre en modo de mantenimiento.

Si usa vSphere Update Manager para actualizar el host, o si trabaja con un clúster de tres hosts, el modo de evacuación predeterminado disponible es **Ensure data accessibility** (Garantizar accesibilidad a los datos). Este modo es más rápido que el modo **Evacuate all data** (Evacuar todos los datos). Sin embargo, el modo **Ensure data accessibility** (Garantizar accesibilidad a los datos) no ofrece protección completa para los datos. Durante un error, es posible que los datos queden expuestos a riesgos y que experimente tiempo de inactividad, además de una pérdida de datos inesperada.

2 Cargue el software en el almacén de datos del host ESXi y compruebe que el archivo esté disponible en el directorio dentro del almacén de datos. Por ejemplo, puede cargar el software en `/vmfs/volumes/<datastore>/VMware-ESXi-6.0.0-1921158-depot.zip`.

3 Ejecute el comando `esxcliinstall -d /vmfs/volumes/53b536fd-34123144-8531-00505682e44d/depot/VMware-ESXi-6.0.0-1921158-depot.zip --no-sig-check`. Use el VIB de software `esxcli` para ejecutar este comando.

Una vez que el host ESXi se haya instalado correctamente, verá el siguiente mensaje:

`The update completed successfully, but the system needs to be rebooted for the changes to be effective.` (La actualización ha finalizado correctamente, pero es necesario reiniciar el sistema para que se apliquen los cambios).

4 Debe reiniciar manualmente el host ESXi desde vSphere Web Client.

a Desplácese hasta el host ESXi en el inventario de vSphere Web Client.

b Haga clic con el botón derecho en el host, seleccione **Power > Reboot** (Encender > Reiniciar), haga clic en **Yes** (Sí) para confirmar y espere hasta que se reinicie el host.

c Haga clic con el botón derecho en el host, seleccione **Connection > Disconnect** (Conexión > Desconectar) y, a continuación, seleccione **Connection > Connect** (Conexión > Conectar) para volver a conectarse al host.

Para actualizar los hosts restantes del clúster, repita este procedimiento para cada host.

Si tiene varios hosts en el clúster de vSAN, puede usar vSphere Update Manager para actualizar los hosts restantes.

5 Salga del modo de mantenimiento.

Qué hacer a continuación

1 (Opcional) Actualice el formato de disco de vSAN. Consulte "Actualizar el formato de disco de vSAN mediante RVC," página 103.

2 Compruebe la licencia del host. En la mayoría de los casos, deberá volver a aplicar la licencia del host. Puede usar vSphere Web Client y vCenter Server para aplicar licencias de hosts. Para obtener información acerca de cómo aplicar licencias de hosts, consulte el documento sobre la *administración de vCenter Server y hosts*.

3 (Opcional) Actualice las máquinas virtuales en los hosts mediante vSphere Web Client o vSphere Update Manager.

Acerca del formato de disco de vSAN

La actualización del formato de disco es opcional. El clúster de vSAN seguirá funcionando correctamente si utiliza una versión de formato de disco anterior.

Para obtener mejores resultados, actualice los objetos para que usen la versión de formato en disco más reciente. El formato en disco más reciente proporciona el conjunto completo de características de vSAN.

Según el tamaño de los grupos de discos, la actualización del formato de disco puede ser lenta, debido a que los grupos de discos se actualizan de a uno por vez. Para cada actualización de grupo de discos, se evacúan todos los datos de cada dispositivo y se quita el grupo de discos del clúster de vSAN. Luego, el grupo de discos vuelve a agregarse a vSAN con el nuevo formato en disco.

NOTA: Una vez que actualice el formato en disco, no podrá revertir el software en los hosts o agregar determinados hosts más antiguos al clúster.

Cuando inicie una actualización del formato en disco, vSAN realizará varias operaciones que puede supervisar desde la página Resincronización de componentes. La tabla resume todos los procesos que se realizan durante la actualización del formato de disco.

Tabla 9-2. Progreso de la actualización

% de finalización	Descripción
0 %-5 %	Comprobación del clúster. Se comprueban y preparan los componentes del clúster para la actualización. Este proceso demora algunos minutos. vSAN comprueba que no existen problemas pendientes que puedan impedir que se complete la actualización. ■ Todos los hosts están conectados. ■ Todos los hosts poseen la versión de software correcta. ■ Todos los discos tienen un estado correcto. ■ Es posible acceder a todos los objetos.
5 %-10 %	Actualización del grupo de discos. vSAN realiza la actualización inicial de los discos sin migración de datos. Este proceso demora algunos minutos.
10 %-15 %	Realineación de objetos. vSAN modifica la distribución de todos los objetos para garantizar que están correctamente alineados. Este proceso puede tardar algunos minutos en un sistema pequeño con pocas instantáneas. Puede demorar varias horas, o incluso días, en un sistema grande con muchas instantáneas, muchas escrituras fragmentadas y varios objetos sin alinear.
15 % - 95 %	Eliminación y reformateo del grupo de discos. Cada grupo de discos se elimina del clúster, se reformatea y se vuelve a agregar al clúster. El tiempo requerido para este proceso puede variar en función de los megabytes asignados y la carga del sistema. La transferencia en un sistema que se encuentra en su capacidad de E/S, o cerca de ella, se realiza lentamente.
95 % - 100 %	Actualización final de la versión de los objetos. Se completa la conversión de los objetos al formato en disco nuevo y la resincronización. El tiempo requerido para este proceso puede variar en función de la cantidad de espacio usado y si está seleccionada la opción **Allow reduced redundancy** (Permitir redundancia reducida).

Durante la actualización, puede supervisar el proceso de la actualización desde vSphere Web Client cuando se desplace a la página Resyncing Components (Resincronización de componentes). Consulte "Supervisar las tareas de resincronización en el clúster de vSAN," página 148. También puede utilizar el comando `vsan.upgrade_status <cluster>` de RVC para supervisar la actualización. Utilice la marca `-r <seconds>` opcional para actualizar el estado de la actualización de forma periódica hasta que presione Ctrl+C. La cantidad mínima de segundos permitida entre cada actualización es 60.

También puede supervisar otras tareas de actualización, como la actualización y la eliminación de dispositivos, desde vSphere Web Client, en el panel Recent Tasks (Tareas recientes) de la barra de estado.

Al actualizar el formato de disco, se aplican las siguientes consideraciones:

- Si se actualiza un clúster con tres hosts y se desea ejecutar una evacuación completa, se generan errores en los objetos con un **Primary level of failures to tolerate** (Nivel principal de errores que se toleran) mayor que cero. Un clúster con tres hosts no puede reproteger un grupo de discos que está siendo totalmente evacuado con los recursos de solo dos hosts. Por ejemplo, cuando el **Nivel primario de errores que se toleran** se establece en 1, vSAN requiere tres componentes de protección (dos reflejos y un testigo); cada componente de protección se ubica en un host separado.

  Para un clúster de tres hosts, se debe seleccionar el modo de evacuación **Ensure data accessibility** (Garantizar accesibilidad a los datos). En este modo, cualquier error de hardware puede producir una pérdida de datos.

  Además, debe asegurarse de disponer de espacio libre suficiente. El espacio debe ser equivalente a la capacidad lógica consumida del grupo de discos más grande. La capacidad debe estar disponible en un grupo de discos independiente del que se va a migrar.

- Cuando se actualiza un clúster con tres hosts o un clúster con recursos limitados, se debe permitir que las máquinas virtuales funcionen en un modo de redundancia reducida. Ejecute el comando de RVC con la opción `vsan.ondisk_upgrade --allow-reduced-redundancy`.

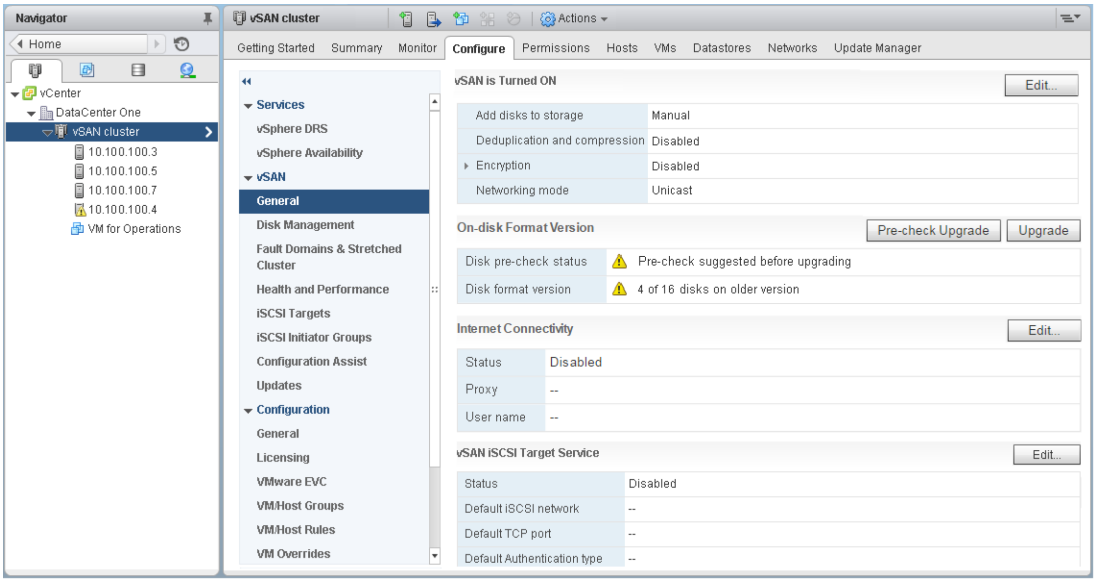
- Si usa la opción de comando `--allow-reduced-redundancy`, es posible que ciertas máquinas virtuales no puedan tolerar errores durante la migración. Esta tolerancia a errores reducida también puede producir pérdida de datos. vSAN restaura la redundancia y el cumplimiento completos una vez finalizada la actualización. Durante la actualización, el estado de cumplimiento de las máquinas virtuales y sus redundancias experimentan un incumplimiento temporal. Una vez que finalizan la actualización y todas las tareas de reconstrucción, las máquinas virtuales pasan a estado de cumplimiento.

- Cuando la actualización se encuentre en progreso, no extraiga ni desconecte ningún host, y no coloque un host en el modo de mantenimiento. Estas acciones podrían provocar errores en la actualización.

Para obtener información sobre los comandos y las opciones de comandos de RVC, consulte la *Guía de referencia de los comandos de RVC*.

Actualizar el formato de disco de vSAN mediante vSphere Web Client

Una vez que haya terminado de actualizar los hosts de vSAN, puede realizar la actualización del formato de disco.



NOTA: Si habilita el cifrado o la desduplicación y la compresión en un clúster de vSAN existente, el formato en disco se actualiza automáticamente a la versión más reciente. Este procedimiento no es obligatorio. Puede evitar reformatear los grupos de discos dos veces. Consulte "Editar la configuración de vSAN," página 52.

Prerequisitos

- Compruebe que esté usando la versión actualizada de vCenter Server.
- Compruebe que esté usando la versión más reciente de los hosts ESXi.
- Compruebe que los discos se encuentren en buen estado. Desplácese hasta la página Disk Management (Administración de discos) en vSphere Web Client para comprobar el estado del objeto.
- Compruebe que los componentes de hardware y software que planea usar estén certificados y aparezcan en el sitio web de la guía de compatibilidad de VMware, a la cual puede acceder mediante la siguiente URL: http://www.vmware.com/resources/compatibility/search.php.
- Compruebe que tenga espacio suficiente para ejecutar la actualización del formato de disco. Ejecute el comando de RVC, `vsan.whatif_host_failures`, para determinar si dispone de capacidad suficiente para completar correctamente la actualización o recompilar los componentes en caso de que haya errores durante la actualización.
- Compruebe que los hosts no estén en modo de mantenimiento. Al actualizar el formato de disco, no coloque los hosts en el modo de mantenimiento. Cuando cualquier host miembro de un clúster de vSAN entra en modo de mantenimiento, la capacidad de recursos disponible se reduce porque el host miembro deja de aportar capacidad al clúster. Es posible que se produzca un error en la actualización del clúster.
- Compruebe que no haya tareas de recompilación de componentes en curso en el clúster de vSAN. Consulte "Supervisar las tareas de resincronización en el clúster de vSAN," página 148.

Procedimiento

1 Desplácese hasta el clúster de vSAN en vSphere Web Client.

2 Haga clic en la pestaña **Configurar**.

3 En vSAN, seleccione **General**.

4 (Opcional) En Versión de formato en disco, haga clic en **Comprobación previa de actualización**.

La comprobación previa de actualización analizará el clúster para detectar problemas que puedan evitar que la actualización se realice correctamente. Algunos de los elementos que se comprueban son el estado del host, el estado del disco, el estado de la red y el estado de los objetos. Los problemas de actualización se muestran en el cuadro de texto **Estado de comprobación previa de disco**.

5 En On-disk Format Version (Versión de formato en disco), haga clic en **Upgrade** (Actualizar).

6 Haga clic en **Sí** en el cuadro de diálogo Actualizar para realizar la actualización del formato en disco.

vSAN realiza un reinicio secuencial de cada grupo de discos del clúster. La columna On-disk Format Version (Versión de formato en disco) muestra la versión del formato de disco de los dispositivos de almacenamiento del clúster. La columna Disks with outdated version (Discos con versión desactualizada) indica la cantidad de dispositivos con el nuevo formato. Cuando la actualización se realice de forma correcta, el valor de Discos con versión desactualizada será 0.

Si ocurre un error durante la actualización, puede consultar la página Resyncing Components (Resincronización de componentes) en vSphere Web Client. Espere a que se complete la resincronización y vuelva a ejecutar la actualización. También puede comprobar el estado del clúster mediante el servicio de estado. Después de resolver cualquier problema que haya surgido a partir de las comprobaciones de estado, puede volver a ejecutar la actualización.

Actualizar el formato de disco de vSAN mediante RVC

Una vez que haya terminado de actualizar los hosts de vSAN, puede usar la herramienta Ruby vSphere Console (RVC) para continuar con la actualización del formato de disco.

Prerequisitos

- Compruebe que esté usando la versión actualizada de vCenter Server.
- Compruebe que la versión de los hosts ESXi que se ejecutan en el clúster de vSAN sea la versión 6.5 o una versión posterior.
- Compruebe que los discos estén en buen estado. Para ello, vaya a la página Disk Management (Administración de discos) en vSphere Web Client. También puede ejecutar el comando de RVC `vsan.disk_stats` para comprobar el estado del disco.
- Compruebe que los componentes de hardware y software que planea usar estén certificados y aparezcan en el sitio web de la Guía de compatibilidad de VMware, en la siguiente URL: http://www.vmware.com/resources/compatibility/search.php.
- Compruebe que tenga espacio suficiente para ejecutar la actualización del formato de disco. Ejecute el comando de RVC `vsan.whatif_host_failures` para determinar si dispone de capacidad suficiente para finalizar en forma correcta la actualización o realizar una reconstrucción de componentes en caso de que haya errores durante la actualización.
- Compruebe que PuTTY o un cliente SSH similar estén instalados para acceder a la herramienta RVC.

  Para obtener información detallada sobre la descarga de la herramienta RVC y sobre el uso de comandos de RVC, consulte la *Guía de referencia de los comandos de RVC*.
- Compruebe que los hosts no estén en modo de mantenimiento. Al actualizar el formato en disco, no coloque los hosts en el modo de mantenimiento. Cuando cualquier host miembro de un clúster de vSAN entra en modo de mantenimiento, la capacidad de recursos disponible se reduce porque el host miembro deja de aportar capacidad al clúster, y es posible que se produzca un error en la actualización del clúster.

- Compruebe que no haya tareas de recompilación de componentes en curso en el clúster de vSAN mediante la ejecución del comando de RVC vsan.resync_dashboard.

Procedimiento

1 Inicie sesión en vCenter Server con la herramienta RVC.

2 Ejecute el comando vsan.disks_stats /< vCenter IP address or hostname>/<data center name>/computers/<cluster name> para ver el estado del disco.

Por ejemplo: vsan.disks_stats /192.168.0.1/BetaDC/computers/VSANCluster

El comando enumera los nombres de todos los dispositivos y los hosts del clúster de vSAN. El comando también muestra el formato de disco actual y su estado de mantenimiento. También puede comprobar el estado actual de los dispositivos de la columna **Health Status** (Estado de mantenimiento) de la página Disk Management (Administración de discos). Por ejemplo, el estado del dispositivo que se muestra es Unhealthy (Estado incorrecto) en la columna **Health Status** (Estado de mantenimiento) para los hosts o los grupos de discos que tienen dispositivos que presentan errores.

3 Ejecute el comando vsan.ondisk_upgrade <path to vsan cluster>.

Por ejemplo: vsan.ondisk_upgrade /192.168.0.1/BetaDC/computers/VSANCluster

4 Supervise el progreso en RVC.

RVC actualiza un grupo de discos a la vez.

Una vez que la actualización del formato de disco finalice correctamente, aparecerá el siguiente mensaje:

```
Done with disk format upgrade phase (Finalizó la fase de actualización del formato de disco)

There are n v1 objects that require upgrade Object upgrade progress: n upgraded, 0 left (Hay n objetos de v1 que requieren una actualización. Progreso de actualización de objetos: n actualizados, 0 restantes)

n upgraded (Finalizó la actualización de objetos: n actualizados)

Done VSAN upgrade (Finalizó la actualización de VSAN)
```

5 Ejecute el comando vsan.obj_status_report para verificar que las versiones de los objetos se actualicen al nuevo formato en disco.

Comprobar la actualización del formato de disco de vSAN

Una vez finalizada la actualización del formato de disco, debe comprobar si el clúster de vSAN está usando el nuevo formato en disco.

Procedimiento

1 Desplácese hasta el clúster de vSAN en vSphere Web Client.

2 Haga clic en la pestaña **Configurar**.

3 En vSAN, haga clic en **Administración de discos**.

La versión actual del formato de disco aparece en la columna Disk Format Version (Versión de formato de disco). Por ejemplo, si usa el formato de disco 2.0, este aparece como la versión 2 en la columna Disk Format Version (Versión de formato de disco). Para el formato en disco 3.0, la versión de formato de disco aparece como la versión 3.

Comprobar la actualización del clúster de vSAN

La actualización del clúster de vSAN no finalizará hasta que compruebe que está usando la versión más reciente de vSphere y que vSAN está disponible para su uso.

Procedimiento

1 Desplácese hasta el clúster de vSAN en vSphere Web Client.

2 Haga clic en la pestaña **Configure** (Configurar) y compruebe que aparezca vSAN.

- También puede desplazarse hasta el host ESXi y seleccionar **Summary** (Resumen) > **Configuration** (Configuración) y comprobar que utiliza la versión más reciente del host ESXi.

Usar las opciones de comandos de actualización de RVC

El comando `vsan.ondisk_upgrade` proporciona diversas opciones de comando que pueden utilizarse para controlar y administrar la actualización del clúster de vSAN. Por ejemplo, puede permitir una redundancia reducida para realizar la actualización cuando tenga un poco de espacio libre disponible.

Ejecute el comando `vsan.ondisk_upgrade --help` para visualizar la lista de las opciones de comandos de RVC.

Use estas opciones de comandos con el comando `vsan.ondisk_upgrade`.

Tabla 9-3. Opciones de comandos de actualización

Opciones	Descripción
`--hosts_and_clusters`	Use esta opción para especificar rutas de acceso a todos los sistemas host del clúster o los recursos informáticos del clúster.
`--ignore-objects, -i`	Use esta opción para omitir la actualización de un objeto de vSAN. También puede usar esta opción de comando para eliminar la actualización de la versión de un objeto. Cuando use esta opción de comando, los objetos continuarán utilizando la versión de formato en disco actual.
`--allow-reduced-redundancy, -a`	Use esta opción para eliminar la necesidad de contar con espacio libre equivalente a un grupo de discos durante la actualización de discos. Con esta opción, las máquinas virtuales funcionan en modo de redundancia reducida durante la actualización, lo que significa que es posible que ciertas máquinas virtuales no toleren errores temporalmente, y esta incapacidad puede producir pérdida de datos. vSAN restaura la redundancia y el cumplimiento completos una vez finalizada la actualización.
`--force, -f`	Use esta opción para permitir forzar el procedimiento y responder automáticamente todas las preguntas de confirmación.
`--help, -h`	Use esta opción para mostrar las opciones de ayuda.

Para obtener información sobre el uso de los comandos de RVC, consulte la *Guía de referencia de los comandos de RVC*.

Recomendaciones de compilación de vSAN para vSphere Update Manager

vSAN genera líneas base del sistema y grupos de líneas base para usarlos con vSphere Update Manager. Puede utilizar estas líneas base recomendadas para actualizar software, revisiones y extensiones de los hosts del clúster de vSAN.

vSAN 6.6.1 y las versiones posteriores generan recomendaciones de compilación automatizadas para los clústeres de vSAN. vSAN combina información de la guía de compatibilidad de VMware y del catálogo de versiones de vSAN con información sobre las versiones de ESXi instaladas. Estas actualizaciones recomendadas proporcionan la mejor versión disponible para asegurarse de que el hardware se mantenga en un estado admitido.

Líneas base del sistema de vSAN

Las recomendaciones de compilación de vSAN se proporcionan a través de las líneas base del sistema de vSAN para Update Manager. vSAN administra estas líneas base del sistema. Son de solo lectura y no se pueden personalizar.

vSAN genera un grupo de líneas base para cada clúster de vSAN. Las líneas base del sistema de vSAN se enumeran en el panel Líneas base de la pestaña Líneas base y grupos. Puede seguir creando y corrigiendo sus propias líneas base.

Update Manager examina cada clúster de vSAN de forma automática para comparar el cumplimiento con el grupo de líneas base. Para actualizar el clúster, debe corregir de forma manual la línea base del sistema mediante Update Manager. Es posible corregir la línea base del sistema de vSAN en un único host o en todo el clúster.

Catálogo de versiones de vSAN

El catálogo de versiones de vSAN contiene información sobre las versiones disponibles, el orden de preferencia de las versiones y las revisiones esenciales necesarias para cada versión. El catálogo de versiones de vSAN se hospeda en VMware Cloud.

vSAN requiere conectividad a Internet para acceder al catálogo de versiones. No es necesario que esté inscrito en el Programa de mejora de la experiencia de cliente (Customer Experience Improvement Program, CEIP) para que vSAN pueda acceder al catálogo de versiones.

Trabajar con las recomendaciones de compilación de vSAN

Update Manager compara las versiones de ESXi instaladas con la información de la lista de compatibilidad de hardware (Hardware Compatibility List, HCL) en la guía de compatibilidad de VMware. Determina la ruta de acceso de actualización correcta para cada clúster de vSAN con base en el catálogo de versiones de vSAN actual. vSAN también incluye las actualizaciones de revisión y los controladores necesarios para la versión recomendada en su línea base del sistema.

Las recomendaciones de compilación de vSAN garantizan que cada clúster de vSAN permanezca en el estado de compatibilidad de hardware actual o superior. Si el hardware en el clúster de vSAN no está incluido en la HCL, vSAN recomienda una actualización a la versión más reciente, ya que no es peor que el estado actual.

Los siguientes ejemplos describen la lógica utilizada por las recomendaciones de compilación de vSAN.

Ejemplo 1 Un clúster de vSAN ejecuta la versión 6.0 Update 2 y su hardware se encuentra en la HCL de la versión 6.0 Update 2. La HCL muestra que el hardware es compatible hasta la versión 6.0 Update 3, pero no para las versiones 6.5 y posteriores. vSAN recomienda una actualización a la versión 6.0 Update 3, incluidas las revisiones esenciales que necesita la versión.

Ejemplo 2 Un clúster de vSAN ejecuta la versión 6.0 Update 2 y su hardware se encuentra en la HCL de la versión 6.0 Update 2. El hardware también se admite en la HCL de la versión 6.5 Update 1. vSAN recomienda una actualización a la versión 6.5 Update 1.

Ejemplo 3 Un clúster de vSAN ejecuta la versión 6.0 Update 2 y su hardware no se encuentra en la HCL de dicha versión. vSAN recomienda una actualización a la versión 6.5 Update 1, a pesar de que el hardware no aparece en la HCL de la versión 6.5 Update 1. vSAN recomienda la actualización porque el nuevo estado no es peor que el estado actual.

El motor de recomendaciones se ejecuta periódicamente (una vez al día) o cuando ocurren los siguientes eventos.

- La pertenencia al clúster cambia. Por ejemplo, cuando se agrega o se quita un host.
- El servicio de administración de vSAN se reinicia.
- Un usuario inicia sesión en My VMware (my.vmware.com) a través de vSphere Client o RVC.
- Se realiza una actualización en la guía de compatibilidad de VMware o en el catálogo de versiones de vSAN.

La comprobación de estado de la recomendación de compilación de vSAN muestra la compilación actual que se recomienda para el clúster de vSAN. También puede avisarle de cualquier problema existente en la función.

Requisitos del sistema

Update Manager debe instalarse manualmente en vCenter Server de Windows.

vSAN requiere acceso a Internet para actualizar los metadatos de la versión, para comprobar la guía de compatibilidad de VMware y para descargar las imágenes ISO desde My VMware.

vSAN requiere credenciales válidas de My VMware (my.vmware.com) con el fin de descargar las imágenes ISO para las actualizaciones. En los hosts que ejecutan la versión 6.0 Update 1 o una anterior, debe usar RVC para introducir las credenciales de My VMware. En los hosts que ejecutan software de una versión posterior, puede iniciar sesión desde la comprobación de estado de la recomendación de compilación de ESX.

Para introducir las credenciales de My VMware desde RVC, ejecute el siguiente comando:
vsan.login_iso_depot -u <*nombre de usuario*> **-p** <*contraseña*>

Administrar dispositivos en un clúster de vSAN 10

Puede realizar varias tareas de administración de dispositivos en un clúster de vSAN. Puede crear grupos de discos híbridos o basados íntegramente en tecnología flash, habilitar vSAN para reclamar dispositivos para memoria caché y capacidad, habilitar o deshabilitar los indicadores LED en los dispositivos, marcar dispositivos como flash, marcar dispositivos remotos como locales, etc.

Este capítulo cubre los siguientes temas:

Administrar grupos de discos y dispositivos

Cuando habilite vSAN en un clúster, seleccione un modo de reclamación de discos para organizar los dispositivos en grupos.

vSAN 6.6 y las versiones posteriores cuentan con un flujo de trabajo uniforme para el reclamo de discos en todos los escenarios. Los discos disponibles se agrupan por modelo y tamaño o por host. Debe seleccionar los dispositivos que destinará para almacenamiento en caché y los que usará para capacidad.

Crear un grupo de discos en un host

Al crear grupos de discos, es necesario especificar manualmente cada host y cada dispositivo que se deseen utilizar para el almacén de datos de vSAN. Organice los dispositivos de almacenamiento en caché y de capacidad en grupos de discos.

Para crear un grupo de discos, debe definir el grupo de discos y seleccionar los dispositivos de forma individual para incluirlos en dicho grupo. Cada grupo de discos contiene un dispositivo flash de almacenamiento en caché y uno o varios dispositivos de capacidad.

Cuando cree un grupo de discos, tenga en cuenta la proporción entre el almacenamiento en caché flash y la capacidad consumida. Si bien la proporción depende de los requisitos y la carga de trabajo del clúster, considere la posibilidad de usar una proporción entre la memoria caché flash y la capacidad consumida de por lo menos un 10 % (sin incluir réplicas como los duplicados).

El clúster de vSAN contiene inicialmente un solo almacén de datos de vSAN con cero bytes consumidos.

A medida que crea grupos de discos en cada host y agrega dispositivos de capacidad y memoria caché, el tamaño del almacén de datos aumenta en función de la cantidad de capacidad física que agregaron estos dispositivos. vSAN crea un solo almacén de datos distribuido de vSAN utilizando la capacidad local vacía que está disponible en los hosts agregados al clúster.

Si el clúster requiere varios dispositivos de almacenamiento en caché flash, deberá crear varios grupos de discos de forma manual, debido a que se permite un máximo de un dispositivo de almacenamiento en caché flash por grupo de discos.

NOTA: Si se agrega un nuevo host ESXi al clúster de vSAN, el almacenamiento local de ese host no se agrega automáticamente al almacén de datos de vSAN. Debe crear un grupo de discos y agregar los dispositivos al grupo de discos para usar el nuevo almacenamiento del nuevo host de ESXi.

Reclamar discos para el clúster de vSAN

Puede seleccionar varios dispositivos de los hosts. vSAN crea grupos de discos predeterminados por usted.

Cuando agrega más capacidad a los hosts o nuevos hosts con capacidad al clúster de vSAN, puede seleccionar los dispositivos nuevos para incrementar la capacidad del almacén de datos de vSAN. En un clúster basado íntegramente en tecnología flash, puede marcar los dispositivos flash para usarlos como capacidad.

Después de que vSAN haya reclamado dispositivos, crea el almacén de datos compartidos de vSAN. El tamaño total del almacén de datos refleja la capacidad de todos los dispositivos de capacidad en los grupos de discos de todos los hosts en el clúster. Para los metadatos, se utilizan algunas sobrecargas de capacidad.

Crear un grupo de discos en un host de vSAN

Puede combinar manualmente dispositivos específicos de almacenamiento en caché y ciertos dispositivos de capacidad para definir grupos de discos en un host en particular.

Con este método, debe seleccionar dispositivos manualmente para crear un grupo de discos para un host. Debe agregar un dispositivo de almacenamiento en caché y, al menos, un dispositivo de capacidad al grupo de discos.

Procedimiento

1. Desplácese hasta el clúster de vSAN en vSphere Web Client.
2. Haga clic en la pestaña **Configurar**.
3. En vSAN, haga clic en **Disk Management** (Administración de discos).
4. Seleccione el host y haga clic en el icono **Create a new disk group** (Crear un nuevo grupo de discos) ().
   - Seleccione el dispositivo flash que se utilizará para el almacenamiento en caché.
   - En el menú desplegable **Capacity type** (Tipo de capacidad), seleccione el tipo de discos de capacidad que desea utilizar, según el tipo de grupo de discos que desea crear (HDD para componentes híbridos o Flash para componentes basados íntegramente en tecnología flash).
   - Seleccione los dispositivos que desea utilizar para capacidad.

5 Haga clic en **OK** (Aceptar).

El nuevo grupo de discos se muestra en la lista.

Reclamar dispositivos de almacenamiento para un clúster de vSAN

Puede seleccionar un grupo de dispositivos de capacidad y de memoria caché. vSAN los organizará en grupos de discos predeterminados.

Procedimiento

1 Desplácese hasta el clúster de vSAN en vSphere Web Client.

2 Haga clic en la pestaña **Configurar**.

3 En vSAN, haga clic en **Disk Management** (Administración de discos).

4 Haga clic en el icono **Claim Disks** (Recuperar discos) ().

5 Seleccione los dispositivos que se agregarán al grupo de discos.

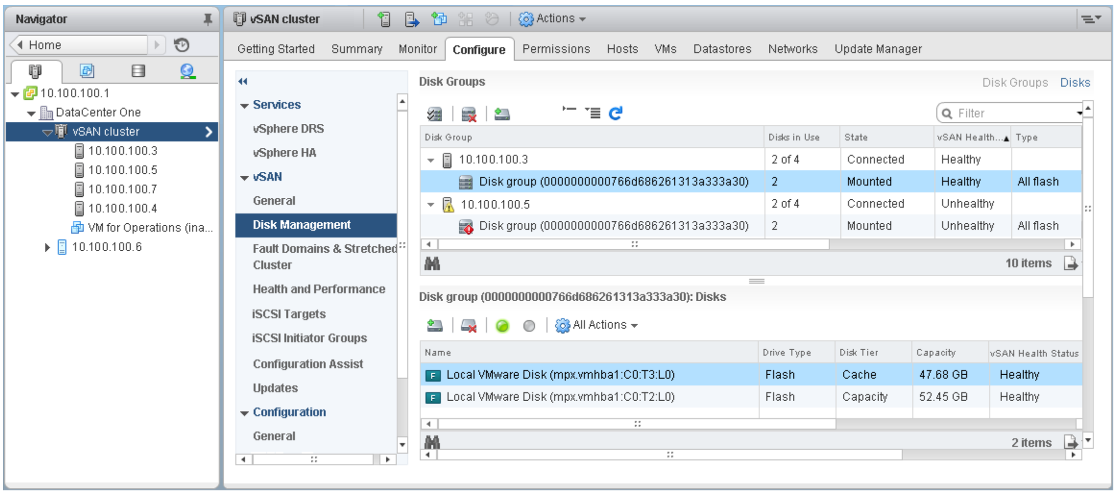
- Cada host que aporte almacenamiento a un grupo de discos híbridos debe aportar un dispositivo de almacenamiento en caché flash y un dispositivo de capacidad, o varios. Puede agregar solamente un dispositivo flash de almacenamiento en caché por grupo de discos.
  - Seleccione un dispositivo flash que se utilizará para almacenamiento en caché y haga clic en el icono **Claim for cache tier** (Recuperar para nivel de almacenamiento en caché) ().
  - Seleccione el dispositivo HDD que se utilizará como dispositivo de capacidad y haga clic en el icono **Claim for capacity tier** (Reclamar para nivel de capacidad) ().
  - Haga clic en **OK** (Aceptar).
- Para los grupos de discos basados íntegramente en tecnología flash, seleccione dispositivos flash tanto para la capacidad como para el almacenamiento en caché.
  - Seleccione un dispositivo flash que se utilizará para almacenamiento en caché y haga clic en el icono **Claim for cache tier** (Recuperar para nivel de almacenamiento en caché) ().
  - Seleccione el dispositivo flash que se utilizará para capacidad y haga clic en el icono **Claim for capacity tier** (Recuperar para nivel de capacidad) ().
  - Haga clic en **OK** (Aceptar).

Para comprobar la función de cada dispositivo agregado al grupo de discos basado íntegramente en tecnología flash, desplácese hasta la columna Disk Role (Función de disco) en la parte inferior de la página Disk Management (Administración de discos). La columna muestra la lista de dispositivos y su función en un grupo de discos.

vSAN reclama los dispositivos seleccionados y los organiza en grupos de discos predeterminados que respaldan el almacén de datos de vSAN.

Trabajar con dispositivos individuales

Puede realizar varias tareas de administración de dispositivos en el clúster de vSAN, como agregar dispositivos a un grupo de discos, eliminar dispositivos de un grupo de discos, habilitar o deshabilitar los LED del localizador y marcar dispositivos.



Agregar dispositivos al grupo de discos

Cuando configura vSAN para reclamar discos en modo manual, puede agregar dispositivos locales adicionales a los grupos de discos existentes.

Los dispositivos deben ser del mismo tipo que los dispositivos existentes en los grupos de discos, como discos de estado sólido (SSD) o discos magnéticos.

Procedimiento

1 Desplácese hasta el clúster de vSAN en vSphere Web Client.

2 Haga clic en la pestaña **Configurar**.

3 En vSAN, haga clic en **Administración de discos**.

4 Seleccione el grupo de discos y haga clic en el icono **Add a disk to the selected disk group** (Agregar un disco al grupo de discos seleccionado) ().

5 Seleccione el dispositivo que desea agregar y haga clic en **OK** (Aceptar).

   Si agrega un dispositivo usado que contiene información de particiones o datos residuales, en primer lugar debe limpiar el dispositivo. Para conocer cuál es el procedimiento para quitar información de particiones de los dispositivos, consulte "Quitar particiones de dispositivos," página 117. También es posible ejecutar el comando de RVC `host_wipe_vsan_disks` para aplicar formato al dispositivo. Para obtener más información sobre los comandos de RVC, consulte la *Guía de referencia de los comandos de RVC*.

Quitar grupos de discos o dispositivos de vSAN

Puede quitar dispositivos seleccionados del grupo de discos o un grupo de discos completo.

Dado que quitar dispositivos no protegidos puede ser un proceso disruptivo para el almacén de datos de vSAN y las máquinas virtuales del almacén de datos, evite quitar dispositivos o grupos de discos.

Por lo general, se quitan dispositivos o grupos de discos de vSAN cuando se actualiza un dispositivo o se reemplaza un dispositivo con errores, o cuando se debe quitar un dispositivo de memoria caché. Otras características de almacenamiento de vSphere pueden usar cualquier dispositivo basado en flash que se quite del clúster de vSAN.

La eliminación permanente de un grupo de discos elimina los miembros del disco y también los datos almacenados en los dispositivos.

NOTA: Al quitar un dispositivo flash de almacenamiento en caché o todos los dispositivos de capacidad de un grupo de discos, se quita el grupo de discos completo.

La evacuación de datos de dispositivos o grupos de discos puede ocasionar un incumplimiento temporal de las directivas de almacenamiento de máquinas virtuales.

Prerequisitos

- Puede poner el host de vSAN en modo de mantenimiento seleccionando la opción **Evacuar todos los datos** o seleccionando **Garantizar accesibilidad a los datos** al eliminar un dispositivo o un grupo de discos. Si selecciona **No data evacuation** (Sin evacuación de datos) en el menú desplegable, es posible que los datos estén en riesgo si ocurre un error durante la evacuación.

Procedimiento

1 Desplácese hasta el clúster de vSAN en vSphere Web Client.

2 Haga clic en la pestaña **Configurar**.

3 En vSAN, haga clic en **Administración de discos**.

4 Quite el grupo de discos o los dispositivos seleccionados.

Opción	Descripción
Remove the Disk Group (Quitar el grupo de discos)	a En Disk Groups (Grupos de discos), seleccione el grupo de discos que desea quitar y haga clic en el icono **Remove the disk group** (). b Seleccione un modo de evacuación de datos.
Remove the Selected Device (Quitar el dispositivo seleccionado)	a En Disk Groups (Grupos de discos), seleccione el grupo de discos que contiene el dispositivo que desea quitar. b En Disks (Discos), seleccione el dispositivo que desea quitar y haga clic en el icono **Remove the selected disk(s) from the disk group** (Quitar disco(s) seleccionado(s) del grupo de discos) (). c Seleccione un modo de evacuación de datos.

Puede transferir los datos evacuados a otro disco u otro grupo de discos del mismo host.

5 Haga clic en **Yes** (Sí) para confirmar.

Los datos se evacúan de los dispositivos seleccionados o de un grupo de discos, y dejan de estar disponibles en vSAN.

Usar los LED del localizador

No puede usar los LED del localizador para identificar la ubicación de los dispositivos de almacenamiento.

vSAN puede encender el LED del localizador en un dispositivo con errores a fin de que pueda identificar fácilmente el dispositivo. Esto resulta especialmente útil al trabajar con varios escenarios de conexión e intercambio en caliente.

Considere utilizar controladoras de almacenamiento de E/S con el modo de paso, debido a que las controladoras con el modo RAID 0 requieren pasos adicionales para habilitar el reconocimiento de las controladoras de los LED del localizador.

Para obtener información sobre la configuración de las controladoras de almacenamiento en modo RAID 0, consulte la documentación del proveedor.

Habilitar y deshabilitar los LED del localizador

Puede activar o desactivar los LED del localizador de los dispositivos de almacenamiento de vSAN. Cuando active el LED del localizador, puede identificar la ubicación de un dispositivo de almacenamiento específico.

Cuando ya no necesite una alerta visual de los dispositivos de vSAN, puede desactivar los LED del localizador en los dispositivos seleccionados.

Prerequisitos

- Compruebe que haya instalado los controladores compatibles para las controladoras de E/S de almacenamiento que habilitan esta característica. Para obtener información sobre los controladores que están certificados por VMware, consulte la *Guía de compatibilidad de VMware* en la URL: http://www.vmware.com/resources/compatibility/search.php.
- En algunos casos, es posible que necesite usar utilidades de otros fabricantes para configurar la característica de los LED del localizador en las controladoras de E/S de almacenamiento. Por ejemplo, al usar HP, debe comprobar que esté instalada la CLI de HP SSA.

Para obtener más información sobre la instalación de VIB de otros fabricantes, consulte el documento *Actualización de vSphere*.

Procedimiento

1. Desplácese hasta el clúster de vSAN en vSphere Web Client.
2. Haga clic en la pestaña **Configurar**.
3. En vSAN, haga clic en **Administración de discos**.
4. Seleccione un host para ver la lista de dispositivos.
5. En la parte inferior de la página, seleccione un dispositivo de almacenamiento o más de la lista, y habilite o deshabilite los LED del localizador en los dispositivos seleccionados.

Opción	Acción
Icono Turns on the locator LED of the selected disk(s) (Activa el LED del localizador del icono de los discos seleccionados)	Habilita el LED del localizador en el dispositivo de almacenamiento seleccionado. Los LED del localizador se pueden habilitar desde la pestaña **Manage** (Administrar) y haciendo clic en **Storage** (Almacenamiento) **>** **Storage Devices** (Dispositivos de almacenamiento).
Icono Turns off the locator LED of the selected disk(s) (Desactiva el LED del localizador de los discos seleccionados)	Deshabilita el LED del localizador en el dispositivo de almacenamiento seleccionado. Los LED del localizador se pueden deshabilitar desde la pestaña **Manage** (Administrar) y haciendo clic en **Storage** (Almacenamiento) **> Storage Devices** (Dispositivos de almacenamiento).

Marcar dispositivos como dispositivos flash

Cuando los hosts ESXi no identifican automáticamente los dispositivos flash como tales, puede marcarlos manualmente como dispositivos flash locales.

Esto también puede ocurrir cuando están habilitados para el modo de RAID 0 y no para el modo de acceso directo. Cuando los dispositivos no se reconocen como dispositivos flash locales, se excluyen de la lista de dispositivos que se ofrecen para vSAN y no es posible utilizarlos en el clúster de vSAN. Cuando estos dispositivos se marcan como dispositivos flash locales, pasan a estar disponibles para vSAN.

Prerequisitos

- Compruebe que el dispositivo sea local para el host.
- Compruebe que el dispositivo no esté en uso.
- Asegúrese de que las máquinas virtuales que acceden al dispositivo estén apagadas y de que el almacén de datos esté desmontado.

Procedimiento

1. Desplácese hasta el clúster de vSAN en vSphere Web Client.
2. Haga clic en la pestaña **Configurar**.
3. En vSAN, haga clic en **Administración de discos**.
4. Seleccione el host para ver la lista de dispositivos disponibles.
5. Desde el menú desplegable **Show** (Mostrar), ubicado en la parte inferior de la página, seleccione **Not in Use** (No en uso).
6. Seleccione un dispositivo flash o más desde la lista y haga clic en el icono **Mark the selected disks as flash disks** (Marcar los discos seleccionados como discos flash) ( ).
7. Haga clic en **Yes** (Sí) para guardar los cambios.

   El tipo de unidad de los dispositivos seleccionados aparece como Flash.

Marcar dispositivos como discos HDD

Cuando los hosts ESXi no identifican automáticamente los discos magnéticos locales como dispositivos HDD, puede marcarlos manualmente como dispositivos HDD locales.

Si ha marcado un disco magnético como dispositivo flash, puede cambiar el tipo de disco del dispositivo marcándolo como disco magnético.

Prerequisitos

- Compruebe que el disco magnético sea local para el host.
- Compruebe que el disco magnético no esté en uso y que esté vacío.
- Compruebe que las máquinas virtuales que acceden al dispositivo estén apagadas.

Procedimiento

1. Desplácese hasta el clúster de vSAN en vSphere Web Client.
2. Haga clic en la pestaña **Configurar**.
3. En vSAN, haga clic en **Administración de discos**.
4. Seleccione el host para ver la lista de dispositivos magnéticos disponibles.
5. Desde el menú desplegable **Show** (Mostrar), ubicado en la parte inferior de la página, seleccione **Not in Use** (No en uso).
6. Seleccione uno o varios discos magnéticos en la lista y haga clic en el icono **Mark the selected disks as HDD disks** (Marcar los discos seleccionados como discos HDD) ( ).
7. Haga clic en **Yes** (Sí) para guardar.

   El tipo de unidad de los discos magnéticos seleccionados aparece como HDD.

Marcar dispositivos como locales

Cuando los hosts usan gabinetes SAS externos, es posible que vSAN reconozca ciertos dispositivos como remotos y que no pueda reclamarlos de manera automática como locales.

En dichos casos, puede indicar que los dispositivos son locales.

Prerequisitos

Asegúrese de que el dispositivo de almacenamiento no sea un dispositivo compartido.

Procedimiento

1. Desplácese hasta el clúster de vSAN en el navegador de vSphere Web Client.
2. Haga clic en la pestaña **Configurar**.
3. En vSAN, haga clic en **Administración de discos**.
4. Seleccione un host para ver la lista de dispositivos.
5. Desde el menú desplegable **Show** (Mostrar), ubicado en la parte inferior de la página, seleccione **Not in Use** (No en uso).
6. Desde la lista de dispositivos, seleccione un dispositivo remoto o varios que desee marcar como locales y haga clic en el icono **Mark the selected disks as local for the host** (Marcar los discos seleccionados como locales para el host).
7. Haga clic en **Yes** (Sí) para guardar los cambios.

Marcar dispositivos como remotos

Los hosts que usan controladores SAS externos pueden compartir dispositivos. Esos dispositivos compartidos pueden marcarse manualmente como remotos, de modo que vSAN no reclame los dispositivos al crear grupos de discos.

En vSAN, no es posible agregar dispositivos compartidos a un grupo de discos.

Procedimiento

1. Desplácese hasta el clúster de vSAN en el navegador de vSphere Web Client.
2. Haga clic en la pestaña **Configurar**.
3. En vSAN, haga clic en **Administración de discos**.
4. Seleccione un host para ver la lista de dispositivos.
5. Desde el menú desplegable **Show** (Mostrar), ubicado en la parte inferior de la página, seleccione **Not in Use** (No en uso).
6. Seleccione un dispositivo o más que desee marcar como remotos y haga clic en el icono **Marks the selected disk(s) as remote for the host** (Marca los discos seleccionados como remotos para el host).
7. Haga clic en **Yes** (Sí) para confirmar.

Agregar un dispositivo de capacidad

Es posible agregar un dispositivo de capacidad a un grupo de discos de vSAN existente.

No es posible agregar dispositivos compartidos a un grupo de discos.

Prerequisitos

Compruebe que el dispositivo no tenga formato y no esté en uso.

Procedimiento

1 Desplácese hasta el clúster de vSAN en vSphere Web Client.

2 Haga clic en la pestaña **Configurar**.

3 En vSAN, haga clic en **Administración de discos**.

4 Seleccione un grupo de discos.

5 Haga clic en el icono **Add a disk to the selected disk group** (Agregar un disco al grupo de discos seleccionado) () ubicado en la parte inferior de la página.

6 Seleccione el dispositivo de capacidad que desea agregar al grupo de discos.

7 Haga clic en **OK** (Aceptar).

El dispositivo se agregará al grupo de discos.

Quitar particiones de dispositivos

Puede quitar la información de particiones de un dispositivo a fin de que vSAN pueda reclamar el dispositivo y utilizarlo.

Si ha agregado un dispositivo que contiene información de particiones o datos residuales, debe quitar toda la información de particiones previa del dispositivo antes de reclamarlo para utilizarlo con vSAN. VMware recomienda agregar dispositivos limpios a los grupos de discos.

Al quitar información de particiones de un dispositivo, vSAN elimina la partición principal que incluye la información de formato del disco y las particiones lógicas del dispositivo.

Prerequisitos

Compruebe que ESXi no esté utilizando el dispositivo como disco de arranque, almacén de datos de VMFS o vSAN.

Procedimiento

1 Desplácese hasta el clúster de vSAN en vSphere Web Client.

2 Haga clic en la pestaña **Configurar**.

3 En vSAN, haga clic en **Administración de discos**.

4 Seleccione un host para ver la lista de dispositivos disponibles.

5 Desde el menú desplegable **Show** (Mostrar), ubicado en la parte inferior de la página, seleccione **Ineligible** (No cumple las condiciones).

6 Seleccione un dispositivo de la lista y haga clic en el icono **Erase partitions on the selected disks** (Borrar particiones de los discos seleccionados) ().

7 Haga clic en **OK** (Aceptar) para confirmar.

El dispositivo se encuentra limpio y no contiene información de particiones.

Expandir y administrar un clúster de vSAN 11

Después de configurar el clúster de vSAN, puede usar vSphere Web Client para agregar hosts y dispositivos de capacidad, quitar hosts y dispositivos, y administrar escenarios de errores.

Este capítulo cubre los siguientes temas:

Expandir un clúster de vSAN

Puede expandir un clúster existente de vSAN agregando hosts o dispositivos a los hosts existentes sin interrumpir las operaciones en curso.

Use uno de los siguientes métodos para expandir el clúster de vSAN.

- Agregue al clúster hosts ESXi nuevos que estén configurados mediante dispositivos compatibles de memoria caché y de capacidad. Consulte "Agregar un host al clúster de vSAN," página 120. Al agregar un dispositivo o un host con capacidad, vSAN no distribuye los datos automáticamente al nuevo dispositivo agregado. Para permitir que vSAN distribuya los datos a los dispositivos agregados recientemente, debe volver a equilibrar manualmente el clúster mediante la herramienta Ruby vSphere Console (RVC). Consulte "Redistribuir de forma manual," página 159.
- Transfiera hosts existentes de ESXi al clúster de vSAN mediante el perfil de host. Consulte "Configurar hosts mediante un perfil de host," página 121. Los nuevos miembros del clúster agregan capacidad informática y de almacenamiento. Debe crear manualmente un subconjunto de grupos de discos a partir de los dispositivos de capacidad locales en el host recién agregado. Consulte "Crear un grupo de discos en un host de vSAN," página 110.

  Verifique que los componentes de hardware, los controladores, el firmware y las controladoras de E/S de almacenamiento que planea usar estén certificados y se enumeren en la Guía de compatibilidad de VMware, en la siguiente URL: http://www.vmware.com/resources/compatibility/search.php. Al agregar dispositivos de capacidad, asegúrese de que los dispositivos no tengan formato ni particiones a fin de que vSAN pueda reconocer y reclamar los dispositivos.
- Agregue nuevos dispositivos de capacidad a hosts ESXi que sean miembros del clúster. Debe agregar el dispositivo manualmente al grupo de discos en el host. Consulte "Agregar dispositivos al grupo de discos," página 112.

Expandir la capacidad y el rendimiento de un clúster de vSAN

Si el clúster de vSAN se está quedando sin capacidad de almacenamiento o si detecta una merma en el rendimiento del clúster, puede expandir la capacidad y el rendimiento del clúster.

- Puede expandir la capacidad de almacenamiento del clúster agregando dispositivos de almacenamiento a los grupos de discos existentes o creando un grupo de discos nuevo. Los grupos de discos nuevos requieren dispositivos flash para la memoria caché. Para obtener información sobre cómo agregar dispositivos a grupos de discos, consulte "Agregar dispositivos al grupo de discos," página 112. Agregar dispositivos de capacidad sin aumentar la memoria caché puede reducir la proporción entre caché y capacidad a un nivel no compatible. Consulte "Consideraciones de diseño para dispositivos flash de almacenamiento en caché en vSAN," página 24.
- Mejore el rendimiento del clúster agregando al menos un dispositivo de almacenamiento en caché (flash) y un dispositivo de capacidad (flash o disco magnético) a una controladora de E/S de almacenamiento existente a o un host de servidor nuevo. Puede agregar uno o varios servidores con grupos de discos adicionales, lo que tiene el mismo impacto en el rendimiento después de que vSAN complete una redistribución proactiva en el clúster de vSAN.

Si bien los hosts únicamente de recursos informáticos pueden existir en un entorno de vSAN y pueden consumir capacidad de otros hosts del clúster, agregue hosts con una configuración uniforme para lograr un funcionamiento correcto.

Para obtener mejores resultados, agregue hosts configurados con dispositivos de almacenamiento en caché y de capacidad. Para obtener información sobre cómo agregar dispositivos a grupos de discos, consulte "Agregar dispositivos al grupo de discos," página 112.

Agregar un host al clúster de vSAN

Puede agregar un host ESXi a un clúster de vSAN en ejecución sin interrumpir las operaciones en curso. Los recursos del host se asocian al clúster.

Prerequisitos

- Compruebe que los recursos, incluidos los controladores, el firmware y las controladoras de E/S de almacenamiento, aparezcan en el sitio web de la Guía de compatibilidad de VMware en http://www.vmware.com/resources/compatibility/search.php.
- VMware recomienda crear hosts configurados de manera uniforme en el clúster de vSAN a fin de que pueda obtener una distribución homogénea de los componentes y los objetos en los dispositivos del clúster. Sin embargo, pueden haber situaciones en las que el clúster no esté equilibrado de manera homogénea, especialmente durante el mantenimiento o si se sobreasigna la capacidad del almacén de datos de vSAN con implementaciones excesivas de máquinas virtuales.

Procedimiento

1. Desplácese hasta el clúster de vSAN en vSphere Web Client.
2. Haga clic con el botón derecho en el clúster y seleccione **Add Host** (Agregar host).
3. Introduzca el nombre del host o la dirección IP y haga clic en **Next** (Siguiente).
4. Introduzca el nombre de usuario y la contraseña asociados con el host y haga clic en **Next** (Siguiente).
5. Consulte la información de resumen y haga clic en **Next** (Siguiente).
6. Asigne una clave de licencia y haga clic en **Next** (Siguiente).

7 (Opcional) Habilite el modo de bloqueo para impedir que los usuarios remotos inicien sesión directamente en el host.

   Puede configurar esta opción en otro momento, editando el perfil de seguridad en la configuración del host.

8 Seleccione lo que desea hacer con las máquinas virtuales y los grupos de recursos del host.

   - **Put this host's virtual machines in the cluster's root resource pool** (Colocar las máquinas virtuales de este host en el grupo de recursos raíz del clúster)

     vCenter Server elimina todos los grupos de recursos del host. Todas las máquinas virtuales de la jerarquía del host están conectadas a la raíz. Las asignaciones de recursos compartidos son relativas a un grupo de recursos, por lo que es posible que deba cambiar los recursos compartidos de una máquina virtual. Hacer este cambio destruye la jerarquía del grupo de recursos.

   - **Create a resource pool for this host's virtual machines and resource pools** (Crear un grupo de recursos para las máquinas virtuales y los grupos de recursos de este host)

     vCenter Server crea un grupo de recursos de nivel superior que se convierte en un elemento secundario directo del clúster y agrega todos los elementos secundarios del host a ese nuevo grupo de recursos. Puede escribir un nombre para ese nuevo grupo de recursos de nivel superior. El valor predeterminado es **Grafted from <host_name>** (Injertado de <nombre_de_host>).

9 Revise la configuración y haga clic en **Finish** (Finalizar).

   El host se agrega al clúster.

Configurar hosts mediante un perfil de host

Cuando se tienen varios hosts en el clúster de vSAN, es posible reutilizar el perfil de un host de vSAN existente y aplicar la configuración del perfil al resto de los hosts del clúster de vSAN.

El perfil de host incluye información sobre la configuración de almacenamiento, la configuración de red y otras características del host. Por lo general, si piensa crear un clúster con una gran cantidad de hosts (por ejemplo, 8, 16, 32 o 64 hosts), utilice la característica de perfil de host para agregar más de un host a la vez al clúster de vSAN.

Prerequisitos

- Compruebe que el host esté en modo de mantenimiento.
- Compruebe que los componentes de hardware, los controladores, el firmware y las controladoras de E/S de almacenamiento se enumeren en la Guía de compatibilidad de VMware en la siguiente URL: http://www.vmware.com/resources/compatibility/search.php.

Procedimiento

1 Cree un perfil de host.

   a Desplácese hasta la vista de Host Profiles.

   b Haga clic en el icono **Extract Profile from a Host** (Extraer perfil de un host) ( ).

   c Seleccione el host que desea utilizar como host de referencia y haga clic en **Next** (Siguiente).

     El host seleccionado debe ser un host activo.

   d Escriba un nombre y una descripción para nuevo perfil y haga clic en **Next** (Siguiente).

   e Revise la información de resumen del nuevo perfil de host y haga clic en **Finish** (Finalizar).

     El nuevo perfil aparece en la lista Host Profile (Perfil del host).

2 Asocie el host al perfil de host deseado.

   a Desde la lista Perfil en la vista de Host Profiles, seleccione el perfil de host que se debe aplicar al host de vSAN.

   b Haga clic en el icono **Attach/Detach Hosts and clusters to a host profile** (Asociar o separar hosts y clústeres para un perfil de host)( ).

   c Seleccione el host desde la lista expandida, haga clic en **Attach** (Asociar) y, a continuación, haga clic en el host que desea asociar con el perfil.

      El host se agrega a la lista Attached Entities (Entidades asociadas).

   d Haga clic en **Next** (Siguiente).

   e Haga clic en **Finish** (Finalizar) para completar la operación de asociación del host con el perfil.

3 Separe del perfil de host el host de vSAN al que se hace referencia.

   Cuando se asocia un perfil de host a un clúster, los hosts de ese clúster también se asocian al perfil de host. Sin embargo, cuando el perfil de host se separa del clúster, la asociación entre el host o los hosts incluidos en el clúster y el perfil de host permanece intacta.

   a Desde la lista Profile (Perfil) en la vista Host Profiles, seleccione el perfil de host que desea separar de un host o un clúster.

   b Haga clic en el icono **Attach/Detach Hosts and clusters to a host profile** (Asociar o separar hosts y clústeres para un perfil de host)( ).

   c Seleccione el host o el clúster desde la lista expandida y haga clic en **Detach** (Separar).

   d Haga clic en **Detach All** (Separar todos) para separar todos los hosts y los clústeres del perfil.

   e Haga clic en **Next** (Siguiente).

   f Haga clic en **Finish** (Finalizar) para completar la operación de desasociación del host del perfil del host.

4 Compruebe que el host de vSAN cumpla con los requisitos del perfil de host asociado y determine si hay parámetros de configuración diferentes a los especificados en el perfil de host.

   a Desplácese hasta un perfil de host.

      En la pestaña **Objects** (Objetos), se enumeran todos los perfiles de host, la cantidad de hosts asociados con el perfil de host y los resultados resumidos de la última comprobación de cumplimiento.

   b Haga clic en el icono **Check Host Profile Compliance** (Comprobar cumplimiento de perfil de host) ( ).

      Para ver detalles específicos sobre qué parámetros tienen diferencias entre el host con incumplimiento y el perfil de host, haga clic en la pestaña **Monitor** (Supervisar) y seleccione la vista Compliance (Cumplimiento). Expanda la jerarquía de objetos y seleccione el host no compatible. Los parámetros con diferencias se muestran en la ventana Compliance (Cumplimiento), debajo de la jerarquía.

      Si se produce un error de cumplimiento, use la acción Remediate (Corregir) para aplicar la configuración del perfil de host al host. Esta acción cambia todos los parámetros administrados por el perfil de host por los valores contenidos en el perfil de host asociado al host.

c Para ver detalles específicos sobre qué parámetros tienen diferencias entre el host con incumplimiento y el perfil de host, haga clic en la pestaña **Monitor** (Supervisar) y seleccione la vista Compliance (Cumplimiento).

d Expanda la jerarquía de objetos y seleccione el host con error.

Los parámetros con diferencias se muestran en la ventana Compliance (Cumplimiento), debajo de la jerarquía.

5 Corrija el host para solucionar los errores de cumplimiento en el host.

a Seleccione la pestaña **Monitor** (Supervisar) y haga clic en **Compliance** (Cumplimiento).

b Haga clic con el botón derecho en los hosts y seleccione **All vCenter Actions (Todas las acciones de vCenter) > Host Profiles (Perfiles de host) > Remediate (Corregir)**.

Puede personalizar el host para actualizar o cambiar los parámetros de entrada del usuario de las directivas de Host Profiles.

c Haga clic en **Next** (Siguiente).

d Revise las tareas necesarias para corregir el perfil de host y haga clic en **Finish** (Finalizar).

El host forma parte del clúster de vSAN y sus recursos están accesibles para el clúster de vSAN. El host también puede acceder a todas las directivas de E/S de almacenamiento de vSAN existentes en el clúster de vSAN.

Trabajar con el modo de mantenimiento

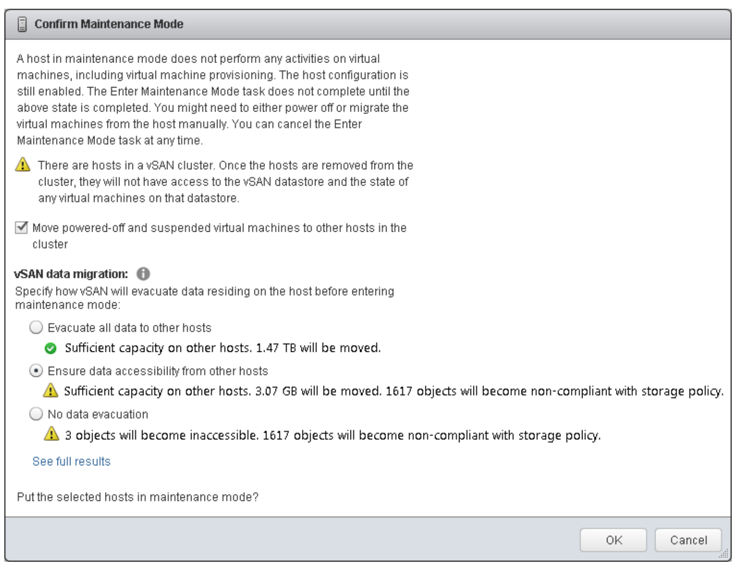
Antes de apagar, reiniciar o desconectar un host que es miembro de un clúster de vSAN, debe poner el host en modo de mantenimiento.

Al trabajar con el modo de mantenimiento, tenga en cuenta las siguientes directrices:

- Cuando se coloca un host ESXi en modo de mantenimiento, se debe seleccionar un modo de evacuación de datos, como **Ensure data accessibility from other hosts** (Garantizar accesibilidad a los datos desde otros hosts) o **Evacuate all data to other hosts** (Evacuar todos los datos a otros hosts).
- Cuando cualquier host miembro de un clúster de vSAN entra en modo de mantenimiento, la capacidad del clúster se reduce de manera automática, ya que el host miembro deja de aportar almacenamiento al clúster.
- Es posible que los recursos informáticos de una máquina virtual no estén en el host que se va a colocar en el modo de mantenimiento, y los recursos de almacenamiento de las máquinas virtuales pueden estar ubicados en cualquier parte del clúster.
- El modo **Ensure data accessibility** (Garantizar accesibilidad a los datos) es más rápido que el modo **Evacuate all data** (Evacuar todos los datos), ya que **Ensure data accessibility** (Garantizar accesibilidad a los datos) solo migra los componentes de los hosts que son imprescindibles para la ejecución de las máquinas virtuales. En este modo, si se experimenta un error, se ve afectada la disponibilidad de la máquina virtual. Cuando se selecciona el modo **Ensure data accessibility** (Garantizar accesibilidad a los datos), los datos no se reprotegen durante un error y puede ocurrir una pérdida de datos inesperada.
- Cuando se selecciona el modo **Evacuate all data** (Evacuar todos los datos), los datos se reprotegen automáticamente contra errores, si hay recursos disponibles y **Primary level of failures to tolerate** (Nivel principal de errores que se toleran) está establecido en 1 o más. En este modo, se migran todos los componentes del host y, según la cantidad de datos que haya en el host, es posible que la migración tarde más. En el modo **Evacuate all data** (Evacuar todos los datos), las máquinas virtuales pueden tolerar errores, incluso durante el mantenimiento planificado.
- Al trabajar con un clúster de tres hosts, no se puede colocar un servidor en el modo de mantenimiento con **Evacuate all data** (Evacuar todos los datos). Para obtener la disponibilidad máxima, debe considerar la posibilidad de diseñar un clúster con cuatro hosts o más.

Antes de colocar un host en el modo de mantenimiento, debe comprobar lo siguiente:

- Si utiliza el modo **Evacuate all data** (Evacuar todos los datos), compruebe que dispone de suficientes hosts y capacidad en el clúster para cumplir con los requisitos de la directiva **Primary level of failures to tolerate** (Nivel principal de errores que se toleran).
- Compruebe que el resto de hosts tenga suficiente capacidad flash para controlar las reservas de Flash Read Cache. Puede ejecutar el comando de RVC `vsan.whatif_host_failures` para analizar el uso de capacidad actual en cada host. Esta información puede ayudarle a determinar si un único error de host puede provocar que el clúster se quede sin espacio, lo que afectaría a la capacidad del clúster, la reserva de memoria caché y los componentes del clúster. Para obtener información sobre los comandos de RVC, consulte la *Guía de referencia de los comandos de RVC*.
- Verifique que disponga de suficientes dispositivos de capacidad en los hosts restantes para controlar los requisitos de la directiva de ancho de las fracciones, si está seleccionada.
- Asegúrese de disponer de suficiente capacidad libre en los hosts restantes para controlar la cantidad de datos que deben migrarse desde el host que va a entrar en modo de mantenimiento.



En el cuadro de diálogo Confirmar modo de mantenimiento se proporciona información para guiarle durante las actividades de mantenimiento. Puede ver el impacto de cada opción de evacuación de datos.

- Si hay o no suficiente capacidad para realizar la operación.
- Cuántos datos se moverán.
- Cuántos objetos dejarán de cumplir con las normas.
- Cuántos objetos se volverán inaccesibles.

Poner un miembro de un clúster de vSAN en modo de mantenimiento

Antes de apagar, reiniciar o desconectar un host que es miembro de un clúster de vSAN, debe poner el host en modo de mantenimiento. Cuando se coloca un host en modo de mantenimiento, se debe seleccionar un modo de evacuación de datos, como **Ensure data accessibility from other hosts** (Garantizar accesibilidad a los datos desde otros hosts) o **Evacuate all data to other hosts** (Evacuar todos los datos a otros hosts).

Cuando cualquier host miembro de un clúster de vSAN entra en modo de mantenimiento, la capacidad del clúster se reduce de manera automática, ya que el host miembro deja de aportar capacidad al clúster.

Prerequisitos

Compruebe que el entorno cuente con las funcionalidades necesarias para la opción seleccionada.

Procedimiento

1. Haga clic con el botón derecho en el host y seleccione **Maintenance Mode > Enter Maintenance Mode** (Modo de mantenimiento > Entrar en modo de mantenimiento).
2. Seleccione un modo de evacuación de datos y haga clic en **OK** (Aceptar).

Opción	Descripción
Garantizar accesibilidad a los datos desde otros hosts	Esta es la opción predeterminada. Al apagar el host o quitarlo del clúster, vSAN se asegura de que todas las máquinas virtuales que están accesibles en este host permanezcan accesibles. Seleccione esta opción si desea quitar el host temporalmente del clúster, por ejemplo, para instalar actualizaciones, y tiene planificado restituir el host en el clúster. Esta opción no es adecuada si se pretende quitar el host del clúster de manera permanente. Por lo general, solamente se requiere una evacuación parcial de datos. Sin embargo, es posible que la máquina virtual ya no cumpla por completo con la directiva de almacenamiento de la máquina virtual durante la evacuación. Eso significa que es posible que no tenga acceso a todas las réplicas. En caso de que se produzca un error mientras el host está en modo de mantenimiento y la directiva **Primary level of failures to tolerate** (Nivel principal de errores que se toleran) esté establecida en 1, es posible que se experimente una pérdida de datos en el clúster. **NOTA:** Este es el único modo de evacuación disponible si se trabaja con un clúster de tres hosts o con un clúster de vSAN configurado con tres dominios de errores.
Evacuar todos los datos a otros hosts	vSAN evacúa todos los datos a los demás hosts del clúster, mantiene o corrige el cumplimiento de la disponibilidad para los componentes afectados, y protege los datos cuando existen recursos suficientes en el clúster. Seleccione esta opción si tiene planificado migrar el host de manera permanente. Al evacuar datos desde el último host del clúster, asegúrese de migrar las máquinas virtuales a otro almacén de datos y luego poner el host en modo de mantenimiento. Este modo de evacuación genera el mayor volumen de transferencia de datos y consume más tiempo y recursos. Todos los componentes del almacenamiento local del host seleccionado se migran a otra ubicación del clúster, de modo que, cuando el host entre en modo de mantenimiento, todas las máquinas virtuales tengan acceso a los componentes de almacenamiento correspondientes sin dejar de cumplir con las directivas de almacenamiento asignadas. **NOTA:** Si un objeto de una máquina virtual que tiene datos en el host no está accesible y no se evacúa por completo, el host no podrá entrar en el modo de mantenimiento.
Sin evacuación de datos	vSAN no evacúa datos de este host. Al apagar el host o quitarlo del clúster, es posible que algunas máquinas virtuales dejen de estar accesibles.

Un clúster con tres dominios de errores tiene las mismas restricciones que un clúster con tres hosts, entre ellas, la imposibilidad de usar el modo **Evacuate all data** (Evacuar todos los datos) o de reproteger los datos después de un error.

Qué hacer a continuación

Puede hacer un seguimiento del progreso de la migración de datos en el clúster. Consulte "Supervisar las tareas de resincronización en el clúster de vSAN," página 148.

Administrar dominios de errores en clústeres de vSAN

Si el clúster de vSAN abarca varios bastidores y chasis de servidores blade en un centro de datos y quiere asegurarse de que los hosts estén protegidos contra errores de los bastidores o los chasis, se pueden crear dominios de errores y agregar uno o varios hosts a cada dominio de errores.

Un dominio de errores consta de uno o varios hosts de vSAN agrupados según su ubicación física en el centro de datos. Cuando están configurados, los dominios de errores permiten a vSAN tolerar errores de bastidores físicos completos, así como errores de un solo host, dispositivo de capacidad, vínculo de red o conmutador de red dedicados a un dominio de errores.

La directiva **Primary level of failures to tolerate** (Nivel principal de errores que se toleran) depende de la cantidad de errores que una máquina virtual se aprovisionó para tolerar. Por ejemplo, cuando una máquina virtual está configurada con el atributo **Nivel primario de errores que se toleran** establecido en 1 (`PFTT = 1`) y usa varios dominios de errores, vSAN puede tolerar un solo error de cualquier tipo y cualquier componente en un dominio de errores, incluido un error de un bastidor completo.

Cuando se configuran dominios de errores en un bastidor y se aprovisiona una máquina virtual nueva, vSAN garantiza que los objetos de protección como las réplicas y los testigos se ubiquen en dominios de errores diferentes. Por ejemplo, si la directiva de almacenamiento de una máquina virtual tiene el atributo **Nivel primario de errores que se toleran** establecido en N (`PFTT = n`), vSAN requiere un mínimo de `2*n+1` dominios de errores en el clúster. Cuando se aprovisionan máquinas virtuales en un clúster con dominios de errores que usan esta directiva, las copias de los objetos asociados de máquinas virtuales se almacenan en bastidores separados.

Se requiere un mínimo de tres dominios de errores. Para obtener mejores resultados, configure cuatro dominios de errores o más en el clúster. Un clúster con tres dominios de errores tiene las mismas restricciones que un clúster con hosts, entre ellas, la imposibilidad de reproteger datos después de un error y de usar el modo **Full data migration** (Migración de datos completa). Para obtener información sobre el diseño y el dimensionamiento de los dominios de errores, consulte "Diseñar y dimensionar dominios de errores de vSAN," página 34.

Piense en un escenario en el cual tiene un clúster de vSAN con 16 hosts. Los hosts se distribuyen entre 4 bastidores (es decir, hay 4 hosts por bastidor). A fin de poder tolerar un error de un bastidor completo, debe crear un dominio de errores para cada bastidor. Es posible configurar un clúster con esa capacidad para tolerar el atributo **Primary level of failures to tolerate** (Nivel principal de errores que se toleran) establecido en 1. Si desea configurar el clúster para permitir máquinas virtuales con el atributo **Primary level of failures to tolerate** (Nivel principal de errores que se toleran) establecido en 2, debe configurar 5 dominios de errores en un clúster.

Cuando se produce un error en un bastidor, todos los recursos, incluida la CPU y la memoria en el bastidor, dejan de estar disponibles en el clúster. Para reducir el impacto de un posible error de un bastidor, debe configurar dominios de errores de tamaños menores. Esto aumenta la cantidad total de la disponibilidad de los recursos en el clúster después de un error de un bastidor.

Al trabajar con dominios de errores, siga las prácticas recomendadas.

- Configure un mínimo de tres dominios de errores en el clúster de vSAN. Para obtener mejores resultados, configure cuatro dominios de errores.
- Un host que no forma parte de ningún dominio de errores se considera que reside en su propio dominio de errores de host individual.
- No es necesario asignar cada host de vSAN a un dominio de errores. Si decide usar dominios de errores para proteger el entorno de vSAN, considere la posibilidad de crear dominios de errores del mismo tamaño.
- Cuando se transfieren a otro clúster, los hosts de vSAN retienen las asignaciones de dominios de errores.

- Al diseñar un dominio de errores, se recomienda configurar dominios de errores con un número de hosts uniforme.

  Para obtener instrucciones sobre el diseño de los dominios de errores, consulte "Diseñar y dimensionar dominios de errores de vSAN," página 34.

- Puede agregar cualquier cantidad de hosts a un dominio de errores. Cada dominio de errores debe contener al menos un host.

Crear un nuevo dominio de errores en un clúster de vSAN

Para garantizar que los objetos de máquinas virtuales sigan ejecutándose correctamente durante un error de un bastidor, puede agrupar los hosts en distintos dominios de errores.

Al aprovisionar una máquina virtual en el clúster con dominios de errores, vSAN distribuye los componentes de protección, como los testigos y las réplicas de los objetos de máquinas virtuales entre distintos dominios de errores. Como consecuencia, el entorno de vSAN puede tolerar errores de bastidores completos, además de errores individuales en un host, en un disco de almacenamiento o en una red.

Prerequisitos

- Elija un nombre único para el dominio de errores. vSAN no admite nombres duplicados de dominios de errores en un clúster.
- Compruebe la versión de los hosts ESXi. Solamente puede incluir hosts de la versión 6.0 o posteriores en los dominios de errores.
- Compruebe que los hosts de vSAN estén conectados. No es posible asignar hosts a un dominio de errores que está sin conexión o que no está disponible debido a un problema de configuración del hardware.

Procedimiento

1. Desplácese hasta el clúster de vSAN en vSphere Web Client.
2. Haga clic en la pestaña **Configurar**.
3. En vSAN, haga clic en **Dominios de errores y clúster ampliado**.
4. Haga clic en el icono **Create a new fault domain** (Crear un nuevo dominio de errores) (+).
5. Escriba el nombre del dominio de errores.
6. Desde el menú desplegable **Show** (Mostrar), seleccione **Hosts not in fault domain** (Hosts no ubicados en dominio de errores) para ver la lista de hosts que no se encuentran asignados a un dominio de errores o seleccione **Show All Hosts** (Mostrar todos los hosts) para ver todos los hosts del clúster.
7. Seleccione un host o más para agregar al dominio de errores.

   Un dominio de errores no puede estar vacío. Debe seleccionar al menos un host para incluir en el dominio de errores.
8. Haga clic en **OK** (Aceptar).

   Los hosts seleccionados aparecen en el dominio de errores.

Transferir hosts al dominio de errores seleccionado

Puede transferir un host a un dominio de errores seleccionado en el clúster de vSAN.

Procedimiento

1. Desplácese hasta el clúster de vSAN en vSphere Web Client.
2. Haga clic en la pestaña **Configurar**.

3. En vSAN, haga clic en **Dominios de errores y clúster ampliado**.
4. Seleccione el dominio de errores y haga clic en el icono **Move hosts into selected fault domain** (Transferir hosts al dominio de errores seleccionado) ( ).
5. En el menú desplegable **Show** (Mostrar), que se encuentra en la parte inferior de la página, seleccione **Hosts not in fault domain** (Hosts no ubicados en dominio de errores) para ver los hosts que están disponibles para agregar a los dominios de errores o seleccione **Show All Hosts** (Mostrar todos los hosts) para ver todos los del clúster.
6. Seleccione el host que desea agregar al dominio de errores.
7. Haga clic en **OK** (Aceptar).

   El host seleccionado aparecen en el dominio de errores.

Transferir hosts a un dominio de errores existente

Puede transferir un host a un dominio de errores existente en el clúster de vSAN.

Procedimiento

1. Desplácese hasta el clúster de vSAN en vSphere Web Client.
2. Haga clic en la pestaña **Configurar**.
3. En vSAN, haga clic en **Fault Domains and Stretched Cluster** (Dominios de errores y clúster ampliado).
4. Seleccione un host o más y haga clic en el icono **Transferir hosts a dominio de errores** ( ).
5. Seleccione un dominio de errores y haga clic en **OK** (Aceptar).

   Cada dominio de errores debe contener al menos un host. Si el host que traslada es el único host del dominio de errores de origen, vSAN eliminará el dominio de errores vacío del clúster.

Transferir hosts fuera de un dominio de errores

Según sus requisitos, puede transferir hosts fuera del dominio de errores.

Prerequisitos

Compruebe que el host esté en línea. No puede mover hosts que están sin conexión o no están disponibles en un dominio de errores.

Procedimiento

1. Desplácese hasta el clúster de vSAN en vSphere Web Client.
2. Haga clic en la pestaña **Configurar**.
3. En vSAN, haga clic en **Dominios de errores y clúster ampliado**.
4. Seleccione el host que desee transferir y haga clic en el icono **Transferir hosts fuera de dominio de errores** ( ).
5. Haga clic en **Yes** (Sí).

   El host seleccionado ya no forma parte del dominio de errores. Cualquier host que no forma parte de un dominio de errores se considera su propio dominio de errores de host individual.

Qué hacer a continuación

Puede agregar hosts a dominios de errores. Consulte "Transferir hosts a un dominio de errores existente," página 128.

Cambiar el nombre de un dominio de errores

Puede cambiar el nombre de un dominio de errores existente en el clúster de vSAN.

Procedimiento

1. Desplácese hasta el clúster de vSAN en vSphere Web Client.
2. Haga clic en la pestaña **Configurar**.
3. En vSAN, haga clic en **Dominios de errores y clúster ampliado**.
4. Seleccione el dominio de errores cuyo nombre desea cambiar y haga clic en el icono **Rename selected fault domain** (Cambiar nombre de dominio de errores seleccionado) ().
5. Introduzca un nombre de dominio de errores.
6. Haga clic en **OK** (Aceptar).

   El nombre nuevo aparecerá en la lista de dominios de errores.

Quitar dominios de errores seleccionados

Cuando ya no necesita un dominio de errores, puede quitarlo del clúster de vSAN.

Procedimiento

1. Desplácese hasta el clúster de vSAN en vSphere Web Client.
2. Haga clic en la pestaña **Configurar**.
3. En vSAN, haga clic en **Dominios de errores y clúster ampliado**.
4. Seleccione el dominio de errores cuyo nombre desea eliminar y haga clic en el icono **Remove selected fault domains** (Quitar dominios de errores seleccionados) ().
5. Haga clic en **Yes** (Sí).

   Se quitan todos los hosts del dominio de errores y se elimina el dominio de errores seleccionado del clúster de vSAN. Se considera que cada host que no forma parte de un dominio de errores reside en su propio dominio de errores de host individual.

Usar el servicio del destino iSCSI de vSAN

Use el servicio del destino iSCSI para habilitar los hosts y las cargas de trabajo físicas que se encuentren fuera del clúster de vSAN para acceder al almacén de datos de vSAN.

Esta característica permite que un iniciador iSCSI en un host remoto transporte datos a nivel de bloque a un destino iSCSI en un dispositivo de almacenamiento del clúster de vSAN.

Tras configurar el servicio del destino iSCSI de vSAN, podrá detectar los destinos iSCSI de vSAN desde un host remoto. Para detectar destinos iSCSI de vSAN, use el puerto TCP del destino iSCSI y la dirección IP de cualquier host del clúster de vSAN. Para garantizar la alta disponibilidad del destino iSCSI de vSAN, configure el soporte de múltiples rutas para la aplicación iSCSI. Puede usar las direcciones IP de dos o más hosts para configurar múltiples rutas.

NOTA: El servicio del destino iSCSI de vSAN no admite otros clientes o iniciadores de vSphere o ESXi, hipervisores de terceros ni migraciones que usen asignaciones de dispositivos sin procesar (raw device mapping, RDM).

El servicio del destino iSCSI de vSAN admite los siguientes métodos de autenticación de CHAP:

CHAP En la autenticación de CHAP, el destino autentica el iniciador, pero el iniciador no autentica el destino.

CHAP mutuo En la autenticación de CHAP mutuo, un nivel adicional de seguridad permite que el iniciador autentique el destino.

Destinos iSCSI

Puede agregar uno o más destinos iSCSI que proporcionen bloques de almacenamiento como números de unidad lógica (logical unit number, LUN). vSAN identifica cada destino iSCSI con un nombre completo de iSCSI (iSCSI qualified Name, IQN) único. Puede usar el IQN para presentar el destino iSCSI a un iniciador iSCSI remoto de modo que este pueda acceder al LUN del destino.

Cada destino iSCSI contiene uno o más LUN. En un clúster de vSAN se define el tamaño de cada LUN, se asigna una directiva de almacenamiento de vSAN a cada LUN y se habilita el servicio del destino iSCSI. Puede configurar una directiva de almacenamiento para usarla como directiva predeterminada del objeto de inicio del servicio del destino iSCSI de vSAN.

Grupos de iniciadores iSCSI

Puede definir un grupo de iniciadores iSCSI que tengan acceso a un destino iSCSI concreto. El grupo de iniciadores iSCSI solo permitirá el acceso de aquellos iniciadores que sean miembros del grupo. Si no define un iniciador o un grupo de iniciadores iSCSI, los iniciadores iSCSI podrán acceder a todos los destinos.

Un nombre único identifica a cada grupo de iniciadores iSCSI. Puede agregar uno o más iniciadores iSCSI como miembros del grupo. Use el IQN del iniciador como nombre del iniciador del miembro.

Habilitar el servicio del destino iSCSI

Antes de crear destinos y LUN iSCSI y definir grupos de iniciadores iSCSI, debe habilitar el servicio del destino iSCSI en el clúster de vSAN.

Procedimiento

1 Desplácese hasta el clúster de vSAN en vSphere Web Client.
2 Haga clic en la pestaña **Configurar**. En vSAN, haga clic en **General**.
3 Haga clic en el botón **Editar** del servicio del destino iSCSI de vSAN.
4 Marque la casilla **Habilitar el servicio del destino iSCSI de vSAN**. Ahora es cuando se pueden seleccionar la red predeterminada, el puerto TCP y el método de autenticación. También puede seleccionar una directiva de almacenamiento de vSAN.
5 Haga clic en **OK** (Aceptar).

Qué hacer a continuación

Tras habilitar el servicio del destino iSCSI, podrá crear destinos y LUN iSCSI, así como definir grupos de iniciadores iSCSI.

Crear un destino iSCSI

Puede crear o editar un destino iSCSI y su LUN asociado.

Prerequisitos

Compruebe que el servicio del destino iSCSI esté habilitado.

Procedimiento

1. Desplácese hasta el clúster de vSAN en vSphere Web Client.
2. Haga clic en la pestaña **Configurar**. En vSAN, haga clic en **Destinos iSCSI**.
3. En la sección Destinos iSCSI de vSAN, haga clic en el icono **Agregar un nuevo destino iSCSI** (+).

   Se abrirá el cuadro de diálogo Nuevo destino iSCSI. El IQN del destino se generará de forma automática.
4. Escriba un alias para el destino. También puede editar la red, el puerto TCP y el método de autenticación del destino.
5. (Opcional) Para definir el LUN del destino, haga clic en la casilla **Agregar el primer LUN al destino iSCSI** e introduzca el tamaño del LUN.
6. Haga clic en **OK** (Aceptar).

Qué hacer a continuación

Defina la lista de iniciadores iSCSI que podrán acceder a este destino.

Agregar un LUN a un destino iSCSI

Puede agregar uno o más LUN a un destino iSCSI, o editar un LUN existente.

Procedimiento

1. Desplácese hasta el clúster de vSAN en vSphere Web Client.
2. Haga clic en la pestaña **Configurar**. En vSAN, haga clic en **Destinos iSCSI**.
3. Seleccione la pestaña **LUN** en la sección de detalles del destino de la página.
4. Haga clic en el icono **Add a new iSCSI LUN to the target** (Agregar un nuevo LUN de iSCSI al destino) (+).

   Se abrirá el cuadro de diálogo Agregar LUN al destino.
5. Introduzca el tamaño del LUN.

   La directiva de almacenamiento de vSAN configurada para el servicio del destino iSCSI se asignará de forma automática. Puede asignar otra directiva a los LUN.
6. Haga clic en **OK** (Aceptar).

Crear un grupo de iniciadores iSCSI

Puede crear un grupo de iniciadores iSCSI para conceder control de acceso a los destinos iSCSI. Solo los iniciadores iSCSI que sean miembros del grupo de iniciadores podrán acceder a los destinos iSCSI.

Procedimiento

1. Desplácese hasta el clúster de vSAN en vSphere Web Client.
2. Haga clic en la pestaña **Configurar**. En vSAN, haga clic en **Grupos de iniciadores iSCSI**.
3. En la sección Grupos de iniciadores iSCSI de vSAN, haga clic en el icono **Agregar un nuevo grupo de iniciadores iSCSI** (+).

   Aparecerá el cuadro de diálogo Nuevo grupo de iniciadores iSCSI de vSAN.
4. Escriba un nombre para el grupo de iniciadores iSCSI.

5 (Opcional) Para agregar miembros al grupo de iniciadores, escriba el IQN de cada miembro.

   Use el siguiente formato para introducir el IQN de los miembros:

   iqn.YYYY-MM.domain:name

   Donde:

   - YYYY = año, como 2016
   - MM = mes, como 09
   - domain = dominio donde se encuentra el iniciador
   - name = nombre del miembro (opcional)

6 Haga clic en **OK** (Aceptar).

Qué hacer a continuación

Agregue miembros al grupo de iniciadores iSCSI.

Asignar un destino a un grupo de iniciadores iSCSI

Puede asignar un destino iSCSI a un grupo de iniciadores iSCSI. Solo los iniciadores que sean miembros del grupo de iniciadores podrán acceder a los destinos asignados.

Prerequisitos

Compruebe que haya un grupo de iniciadores iSCSI.

Procedimiento

1 Desplácese hasta el clúster de vSAN en vSphere Web Client.

2 Haga clic en la pestaña **Configurar**. En vSAN, haga clic en **Grupos de iniciadores iSCSI**.

3 En la sección de detalles del grupo, seleccione la pestaña **Destinos accesibles**.

4 Haga clic en el icono **Add a new accessible target for iSCSI Initiator group** (Agregar un nuevo destino accesible para el grupo de iniciadores iSCSI) (✚[Crear licencia]).

   Se abrirá el cuadro de diálogo Permitir el acceso del grupo de iniciadores al destino.

5 En la pestaña **Filtro**, seleccione un destino de la lista de destinos disponibles.

   La pestaña Objetos seleccionados mostrará los destinos seleccionados actualmente.

6 Haga clic en **OK** (Aceptar).

Supervisar el servicio del destino iSCSI de vSAN

Puede supervisar el servicio del destino iSCSI para ver la colocación física de los componentes del destino iSCSI, así como para comprobar los componentes con errores. También puede supervisar el estado de mantenimiento del servicio del destino iSCSI.

Prerequisitos

Compruebe que se haya habilitado el servicio del destino iSCSI de vSAN y que se hayan creado los destinos y los LUN.

Procedimiento

1 Desplácese hasta el clúster de vSAN en el navegador de vSphere Web Client.

2 Haga clic en **Supervisar** y seleccione **vSAN**.

3 Haga clic en **Destinos iSCSI**.

Los destinos y los LUN iSCSI aparecerán en la parte superior de la página.

4 Haga clic en un alias de destino para ver su estado.

La pestaña Colocación de discos físicos de la parte inferior de la página muestra el lugar donde se encuentran los componentes de datos del destino. La pestaña Errores de cumplimiento muestra los componentes con errores.

5 Haga clic en un LUN para ver su estado.

La pestaña Colocación de discos físicos de la parte inferior de la página muestra el lugar donde se encuentran los componentes de datos del destino. La pestaña Errores de cumplimiento muestra los componentes con errores.

Migrar un clúster híbrido de vSAN a un clúster basado íntegramente en tecnología flash

Puede migrar los grupos de discos de un clúster híbrido de vSAN a grupos de discos basados íntegramente en tecnología flash.

El clúster híbrido de vSAN usa discos magnéticos para la capa de capacidad, y dispositivos flash para la capa de memoria caché. Puede cambiar la configuración de los grupos de discos del clúster de modo que se usen dispositivos flash en la capa de memoria caché y la capa de capacidad.

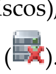
Procedimiento

1 Desplácese hasta el clúster de vSAN en vSphere Web Client.

2 Quite los grupos de discos híbridos de los hosts del clúster.

a Haga clic en la pestaña **Configurar**.

b En vSAN, haga clic en **Administración de discos**.

c En Disk Groups (Grupos de discos), seleccione el grupo de discos que desea quitar y haga clic en el icono **Remove the disk group** ().

d Seleccione **Migración de datos completa** como modo de migración y haga clic en **Sí**.

3 Quite los discos HDD físicos del host.

4 Agregue los dispositivos flash al host.

Compruebe que no haya particiones en los dispositivos flash.

5 Cree los grupos de discos basados íntegramente en tecnología flash en los hosts.

Apagar un clúster de vSAN

Puede apagar un clúster de vSAN.

Prerequisitos

Si la máquina virtual de vCenter Server se ejecuta en el clúster de vSAN, mígrela al primer host, o registre el host donde se ejecuta actualmente.

Procedimiento

1 Apague todas las máquinas virtuales que se ejecuten en el clúster de vSAN.

La máquina virtual de vCenter Server se debe apagar en último lugar.

2 Coloque todos los hosts ESXi que formen parte del clúster en modo de mantenimiento.

Ejecute el comando `esxcli` para establecer el modo de vSAN a fin de pasar al estado de mantenimiento.

```
esxcli system maintenanceMode set –e true –m noAction
```

3 Apague los hosts ESXi.

Usar las directivas de vSAN 12

Al usar vSAN, puede definir requisitos de almacenamiento de máquinas virtuales, como el rendimiento y la disponibilidad, mediante una directiva. vSAN garantiza que a cada máquina virtual implementada en los almacenes de datos de vSAN se le asigne, al menos, una directiva de almacenamiento.

Una vez asignados, los requisitos de la directiva de almacenamiento se traspasan a la capa de vSAN cuando se crea una máquina virtual. El dispositivo virtual se distribuye en el almacén de datos de vSAN para cumplir con los requisitos de rendimiento y disponibilidad.

vSAN utiliza proveedores de almacenamiento para suministrar información sobre el almacenamiento subyacente a vCenter Server. Esta información ayuda a tomar las decisiones adecuadas sobre la selección de máquinas virtuales y a supervisar el entorno de almacenamiento.

Este capítulo cubre los siguientes temas:

Acerca de las directivas de vSAN

Las directivas de almacenamiento de vSAN definen los requisitos de almacenamiento para las máquinas virtuales. Estas directivas determinan cómo los objetos de almacenamiento de máquinas virtuales se aprovisionan y asignan dentro del almacén de datos para garantizar el nivel de servicio requerido.

Al habilitar vSAN en un clúster del host, se crea un solo almacén de datos de vSAN y, asimismo, se asigna una directiva de almacenamiento predeterminada al almacén de datos.

Cuando se conocen los requisitos de almacenamiento de las máquinas virtuales, es posible crear una directiva de almacenamiento que hace referencia a las funcionalidades que anuncia el almacén de datos. Puede crear varias directivas para capturar distintos tipos o distintas clases de requisitos.

Se asigna a cada máquina virtual implementada en los almacenes de datos de vSAN al menos una directiva de almacenamiento de máquinas virtuales. Puede asignar estas directivas de almacenamiento al crear o editar máquinas virtuales.

NOTA: Si no asigna una directiva de almacenamiento a una máquina virtual, vSAN asigna una directiva predeterminada. La directiva predeterminada tiene la opción **Primary level of failures to tolerate** (Nivel principal de errores que se toleran) configurada en 1, una sola fracción de disco por objeto y un disco virtual con aprovisionamiento fino.

El objeto de intercambio de máquina virtual y el objeto de memoria de instantáneas de máquina virtual no cumplen con las directivas de almacenamiento asignadas a una máquina virtual. Estos objetos se configuran con la opción **Primary level of failures to tolerate** (Nivel principal de errores que se toleran) en 1. Es posible que la disponibilidad de estos objetos no sea igual a la de otros objetos que tengan asignada una directiva con un valor diferente para **Primary level of failures to tolerate** (Nivel principal de errores que se toleran).

Tabla 12-1. Atributos de la directiva de almacenamiento

Funcionalidad	Descripción
Number of disk stripes per object (Número de fracciones de disco por objeto)	El número mínimo de dispositivos de capacidad entre los que se fracciona cada réplica de un objeto de una máquina virtual. Un valor mayor que 1 produce un mejor rendimiento, pero también un mayor uso de los recursos del sistema. El valor predeterminado es 1 y el máximo es 12. No cambie el valor de fraccionamiento predeterminado. En un entorno híbrido, las fracciones de discos se distribuyen entre discos magnéticos. En el caso de una configuración basada íntegramente en tecnología flash, el fraccionamiento será entre los dispositivos flash que confirman la capa de capacidad. Asegúrese de que el entorno de vSAN tenga suficientes dispositivos de capacidad presentes para adecuarse a la solicitud.
Flash read cache reservation (Reserva de Flash Read Cache)	La capacidad flash reservada como memoria caché de lectura para el objeto de la máquina virtual. Se especifica como un porcentaje del tamaño lógico del objeto del disco de la máquina virtual (vmdk). La capacidad flash reservada no puede ser utilizada por otros objetos. La capacidad flash no reservada se comparte de manera equitativa entre todos los objetos. Utilice esta opción solamente para solucionar problemas de rendimiento específicos. No es necesario establecer una reserva para obtener memoria caché. La configuración de las reservas de memoria caché de lectura podría ocasionar problemas cuando se transfiere el objeto de la máquina virtual, debido a que los ajustes de reserva de la memoria caché siempre se incluyen con el objeto. El atributo de la directiva de almacenamiento de reserva de Flash Read Cache solo es compatible con las configuraciones híbridas. No se debe usar este atributo al definir una directiva de almacenamiento de máquina virtual para un clúster basado íntegramente en tecnología flash. El valor predeterminado es 0 %. El valor máximo es 100 %. **NOTA:** Como opción predeterminada, vSAN asigna memoria caché de lectura de manera dinámica a los objetos de almacenamiento en función de la demanda. Esta característica representa el uso más flexible y más óptimo de los recursos. Como consecuencia, por lo general, no es necesario cambiar el valor predeterminado de 0 para este parámetro. Si desea aumentar el valor en el momento de solucionar un problema de rendimiento, sea cuidadoso. El sobreaprovisionamiento de reservas de memoria caché entre varias máquinas virtuales puede implicar un desperdicio de espacio en el dispositivo flash por reservas excesivas. Estas reservas de memoria caché no se pueden usar para atender las cargas de trabajo para las que se necesita espacio en cierto momento. Este desperdicio de espacio y falta de disponibilidad podrían causar una degradación en el rendimiento.

Tabla 12-1. Atributos de la directiva de almacenamiento (Continua)

Funcionalidad	Descripción
Nivel primario de errores que se toleran	Define el número de errores de dispositivos y hosts que se pueden tolerar en un objeto de una máquina virtual. Para errores `n` tolerados, cada dato escrito se almacena en las ubicaciones `n+1`, incluidas las copias de paridad si se utiliza RAID 5 o RAID 6. Al aprovisionar una máquina virtual, si no selecciona una directiva de almacenamiento, vSAN asigna esta directiva como la directiva de almacenamiento predeterminada de la máquina virtual. Si se configuran dominios de errores, se requieren `2n+1` dominios de errores con hosts que aporten capacidad. Un host que no forma parte de ningún dominio de errores se considera su propio dominio de errores de host individual. El valor predeterminado es 1. El valor máximo es 3. **NOTA:** Si no desea que vSAN proteja una sola copia reflejada de objetos de máquina virtual, puede establecer el valor de **Nivel primario de errores que se toleran** en 0. Sin embargo, es posible que el host experimente demoras inusuales al entrar en el modo de mantenimiento. Los retrasos ocurren porque vSAN debe evacuar el objeto del host para que la operación de mantenimiento se complete correctamente. Si se establece **Nivel primario de errores que se toleran** en 0, los datos quedan desprotegidos y es posible que se pierdan datos cuando el clúster de vSAN experimente un error de dispositivo. **NOTA:** Si se crea una directiva de almacenamiento y no se especifica un valor para **Nivel primario de errores que se toleran**, vSAN crea una sola copia reflejada de los objetos de máquina virtual. IT puede tolerar un solo error. Sin embargo, si ocurren varios errores de componentes, los datos podrían estar en riesgo. En un clúster ampliado, define el número de errores de dispositivos y hosts que se pueden tolerar en un objeto de máquina virtual. Es posible usar **Primary level of failures to tolerate** (Nivel primario de errores que se toleran) con **Secondary level of failures to tolerate** (Nivel secundario de errores que se toleran) para proporcionar protección local contra errores en objetos dentro de un solo sitio.
Nivel secundario de errores que se toleran	En un clúster ampliado, esta regla define el número de errores de hosts y objetos que se pueden tolerar en un objeto de máquina virtual dentro de un solo sitio. El valor predeterminado es 1. El valor máximo es 3.
Afinidad	En un clúster ampliado, esta regla solo se encuentra disponible si el atributo **Primary level of failures to tolerate** (Nivel primario de errores que se toleran) se configura en 0. Es posible configurar la regla de compatibilidad en **None** (Ninguno), **Preferred** (Preferido) o **Secondary** (Secundario). Esta regla permite limitar los objetos de máquina virtual a un sitio seleccionado en el clúster ampliado. El valor predeterminado es None (Ninguno).
Force provisioning (Forzar aprovisionamiento)	Si la opción se establece en **Yes** (Sí), el objeto se aprovisiona incluso cuando el almacén de datos no puede satisfacer las directivas **Primary level of failures to tolerate** (Nivel principal de errores que se toleran), **Number of disk stripes per object** (Número de fracciones de disco por objeto) y **Flash read cache reservation** (Reserva de Flash Read Cache) especificadas en la directiva de almacenamiento. Use este parámetro en escenarios de arranque y durante una interrupción cuando el aprovisionamiento estándar ya no sea posible. El valor predeterminado **No** es aceptable para la mayoría de los entornos de producción. vSAN no aprovisiona una máquina virtual cuando no se cumplen los requisitos de la directiva; sin embargo, crea correctamente la directiva de almacenamiento definida por el usuario.

Tabla 12-1. Atributos de la directiva de almacenamiento (Continua)

Funcionalidad	Descripción
Reserva de espacio de objetos	Porcentaje del tamaño lógico del objeto del disco de la máquina virtual (vmdk) que se debe reservar o que debe tener aprovisionamiento grueso al implementar máquinas virtuales. El valor predeterminado es 0 %. El valor máximo es 100 %.
Disable object checksum (Deshabilitar suma de comprobación de objetos)	Si la opción se establece en **No**, el objeto calcula la información de suma de comprobación para garantizar la integridad de sus datos. Si esta opción se establece en **Yes** (Sí), el objeto no calcula la información de suma de comprobación. vSAN utiliza la suma de comprobación de extremo a extremo para garantizar la integridad de los datos confirmando que cada copia de un archivo sea exactamente igual que el archivo de origen. El sistema comprueba la validez de los datos durante las operaciones de lectura/escritura y, si se detecta un error, vSAN repara los datos o informa del error. Si se detecta una discrepancia en la suma de comprobación, vSAN repara automáticamente los datos sobrescribiendo los datos incorrectos con los datos correctos. Se realiza el cálculo de la suma de comprobación y la corrección de errores como operaciones en segundo plano. La configuración predeterminada para todos los objetos del clúster es **No**, lo que significa que la suma de comprobación está habilitada.
Failure tolerance method (Método de tolerancia ante errores)	Especifica si el método de replicación de datos optimiza el rendimiento o la capacidad. Si selecciona **RAID-1 (reflejo): rendimiento**, vSAN utiliza más espacio de disco para colocar los componentes de los objetos, pero proporciona un mejor rendimiento para acceder a los objetos. Si selecciona **RAID-5/6 (codificación de borrado): capacidad**, vSAN utiliza menos espacio de disco, pero se reduce el rendimiento. Puede utilizar RAID 5 aplicando el atributo **RAID-5/6 (Erasure Coding) - Capacity** (RAID-5/6 [codificación de borrado]: capacidad) a los clústeres con cuatro o más dominios de errores y establecer **Primary level of failures to tolerate** (Nivel principal de errores que se toleran) en 1. Puede utilizar RAID 6 aplicando el atributo **RAID-5/6 (Erasure Coding) - Capacity** (RAID-5/6 [codificación de borrado]: capacidad) a los clústeres con seis o más dominios de errores y establecer **Primary level of failures to tolerate** (Nivel principal de errores que se toleran) en 2. En los clústeres ampliados con la opción **Secondary level of failures to tolerate** (Nivel secundario de errores que se toleran) configurada, esta regla solo se aplica a **Secondary level of failures to tolerate**. Para obtener más información sobre RAID 5 o RAID 6, consulte "Usar la codificación de borrado RAID 5 o RAID 6," página 80.
IOPS limit for object (Límite de IOPS para objeto)	Define el límite de IOPS para un objeto, como VMDK. El valor de IOPS se calcula como el número de operaciones de E/S, utilizando un tamaño ponderado. Si el sistema utiliza el tamaño de base predeterminado de 32 KB, una E/S de 64 KB representa dos operaciones de E/S. Al calcular las IOPS, la lectura y escritura se consideran equivalentes, pero no se consideran la proporción de aciertos de la memoria caché ni la secuencialidad. Si las IOPS de un disco exceden el límite, se aceleran las operaciones de E/S. Si **IOPS limit for object** (Límite de IOPS para objeto) se establece en 0, no se aplicarán los límites de IOPS. vSAN permite que el objeto duplique la tasa del límite de E/S por segundo durante el primer segundo de la operación o después de un período de inactividad.

Al trabajar con directivas de almacenamiento de máquinas virtuales, debe comprender la manera en que las funcionalidades de almacenamiento afectan al consumo de la capacidad de almacenamiento en el clúster de vSAN. Para obtener más información sobre las consideraciones de diseño y dimensionamiento de las directivas de almacenamiento, consulte Capítulo 3, "Diseñar y dimensionar un clúster de vSAN," página 21.

Ver los proveedores de almacenamiento de vSAN

Al habilitar vSAN, automáticamente se configura y se registra un proveedor de almacenamiento para cada host del clúster de vSAN.

Los proveedores de almacenamiento de vSAN son componentes de software integrados que comunican las funcionalidades del almacén de datos a vCenter Server. Una funcionalidad de almacenamiento está generalmente representada por un par clave/valor, donde la clave es la propiedad específica ofrecida por el almacén de datos. El valor es un número o rango que el almacén de datos puede proporcionar para un objeto aprovisionado, como un objeto del espacio de nombres del directorio principal de la máquina virtual o un disco virtual. También puede usar etiquetas para crear funcionalidades de almacenamiento definidas por el usuario y hacer referencia a ellas al definir una directiva de almacenamiento para una máquina virtual. Para obtener más información sobre cómo aplicar y utilizar etiquetas con los almacenes de datos, consulte la documentación de *Almacenamiento de vSphere*.

Los proveedores de almacenamiento de vSAN informan de un conjunto de funcionalidades de almacenamiento subyacentes a vCenter Server. Asimismo, se comunican con la capa de vSAN para informar de los requisitos de almacenamiento de las máquinas virtuales. Para obtener más información sobre proveedores de almacenamiento, consulte el documento *Almacenamiento de vSphere*.

vSAN registra un proveedor de almacenamiento separado para cada host del clúster de vSAN, mediante la siguiente dirección URL:

http://*host_ip*:8080/version.xml

donde *host_ip* es la dirección IP real del host.

Compruebe que los proveedores de almacenamiento estén registrados.

Procedimiento

1 Desplácese hasta vCenter Server en el navegador de vSphere Web Client.

2 Haga clic en la pestaña **Configurar** y, a continuación, en **Proveedores de almacenamiento**.

Los proveedores de almacenamiento para vSAN se muestran en la lista. Cada host posee un proveedor de almacenamiento, pero solo uno está activo. Los proveedores de almacenamiento que pertenecen a los demás hosts están en espera. Si el host que actualmente posee el proveedor de almacenamiento activo presenta un error, se vuelve activo el proveedor de almacenamiento de otro host.

NOTA: No es posible eliminar del registro de forma manual a los proveedores de almacenamiento que utiliza vSAN. Si es necesario quitar los proveedores de almacenamiento de vSAN o eliminarlos del registro, quite los hosts correspondientes del clúster de vSAN y luego vuelva a agregarlos. Asegúrese de que haya al menos un proveedor de almacenamiento activo.

Acerca de la directiva de almacenamiento predeterminada de vSAN

vSAN requiere que a las máquinas virtuales implementadas en los almacenes de datos de vSAN se les asigne, al menos, una directiva de almacenamiento. Al aprovisionar una máquina virtual, si no le asigna una directiva de almacenamiento de manera explícita, se le asigna la directiva de almacenamiento predeterminada de vSAN.

La directiva predeterminada contiene conjuntos de reglas de vSAN y un conjunto de funcionalidades básicas de almacenamiento, que, por lo general, se usan para ubicar las máquinas virtuales implementadas en los almacenes de datos de vSAN.

Tabla 12-2. Especificaciones de la directiva de almacenamiento predeterminada de vSAN

Especificación	Configuración
Nivel primario de errores que se toleran	1
Number of disk stripes per object (Número de fracciones de disco por objeto)	1
Flash read cache reservation, or flash capacity used for read cache (Reserva de Flash Read Cache o capacidad flash utilizada para la memoria caché de lectura)	0
Reserva de espacio de objetos	0 **NOTA:** Cuando la reserva de espacio de objetos se configura en 0, el disco virtual se aprovisiona con formato fino, de forma predeterminada.
Force provisioning (Forzar aprovisionamiento)	No

Si desea revisar las opciones de configuración de la directiva de almacenamiento predeterminada de máquina virtual desde vSphere Web Client, desplácese hasta **Directivas de almacenamiento de VM** > **Directiva de almacenamiento predeterminada de Virtual SAN** > **Administrar** > **Conjunto de reglas 1: VSAN**.

Para obtener mejores resultados, considere la posibilidad de crear y usar sus propias directivas de almacenamiento de máquina virtual, aunque los requisitos de la directiva sean iguales a los definidos en la directiva de almacenamiento predeterminada. Para obtener información sobre cómo crear una directiva de almacenamiento de máquina virtual definida por el usuario, consulte "Definir una directiva de almacenamiento de máquinas virtuales para vSAN," página 142.

Cuando se asigna una directiva de almacenamiento definida por el usuario como la directiva predeterminada para un almacén de datos, vSAN elimina de manera automática la asociación con la directiva de almacenamiento predeterminada y aplica los ajustes de configuración de la directiva de almacenamiento definida por el usuario en el almacén de datos especificado. En cualquier momento dado, puede asignar una sola directiva de almacenamiento de máquina virtual como la directiva predeterminada para el almacén de datos de vSAN.

Características

Las características siguientes se aplican a la directiva de almacenamiento predeterminada de vSAN.

- La directiva de almacenamiento predeterminada de vSAN se asigna a todos los objetos de máquinas virtuales si no se selecciona ninguna otra directiva de vSAN cuando se aprovisiona una máquina virtual, es decir, cuando el campo **Directiva de almacenamiento de máquina virtual** está configurado como **Valor predeterminado de almacén de datos** en la página Seleccionar almacenamiento. Para obtener más información sobre el uso de las directivas de almacenamiento, consulte el documento *Almacenamiento de vSphere*.

  NOTA: Los objetos de intercambio de máquina virtual y de memoria de máquina virtual reciben la directiva de almacenamiento de vSAN predeterminada cuando **Forzar aprovisionamiento** se establece en **Sí**.

- La directiva predeterminada de vSAN solo se aplica a los almacenes de datos de vSAN. No es posible aplicar la directiva de almacenamiento predeterminada a almacenes de datos no pertenecientes a vSAN (por ejemplo, un almacén de datos de NFS o VMFS).
- Debido a que la directiva de almacenamiento predeterminada de la máquina virtual es compatible con cualquier almacén de datos de vSAN en vCenter Server, puede transferir los objetos de máquinas virtuales aprovisionados con la directiva predeterminada a cualquier almacén de datos de vSAN en vCenter Server.

- Puede clonar la directiva predeterminada y usarla como plantilla para crear una directiva de almacenamiento definida por el usuario.
- Si tiene el privilegio Perfil de almacenamiento.Vista, puede editar la directiva predeterminada. Debe tener al menos un clúster habilitado para vSAN que contenga un host como mínimo. VMware recomienda especialmente no editar los ajustes de configuración de la directiva de almacenamiento predeterminada.
- No es posible editar el nombre ni la descripción de la directiva predeterminada, ni tampoco la especificación del proveedor de almacenamiento de vSAN. Todos los demás parámetros, incluidas las reglas de la directiva, pueden editarse.
- No es posible eliminar la directiva predeterminada.
- La directiva de almacenamiento predeterminada se asigna cuando la directiva que asigna durante el aprovisionamiento de máquinas virtuales no incluye reglas específicas para vSAN.

Asignar una directiva de almacenamiento predeterminada a almacenes de datos de vSAN

Puede asignar una directiva de almacenamiento definida por el usuario como la directiva predeterminada a un almacén de datos a fin de poder volver a utilizar una directiva de almacenamiento que coincida con sus requisitos.

Prerequisitos

Compruebe que la directiva de almacenamiento de máquina virtual que desea asignar como la directiva predeterminada para el almacén de datos de vSAN cumpla con los requisitos de las máquinas virtuales del clúster de vSAN.

Procedimiento

1. Desplácese hasta el almacén de datos de vSAN en vSphere Web Client.
2. Haga clic en la pestaña **Configurar**.
3. En General, haga clic en el botón **Editar** para la directiva de almacenamiento predeterminada y seleccione la directiva de almacenamiento que desea asignar como la predeterminada para el almacén de datos de vSAN.

   vSphere Web Client mostrará una lista de directivas de almacenamiento compatibles con el almacén de datos de vSAN, como la directiva de almacenamiento predeterminada de vSAN y las directivas de almacenamiento definidas por el usuario que tienen definidos conjuntos de reglas de vSAN.
4. Seleccione una directiva y haga clic en **OK** (Aceptar).

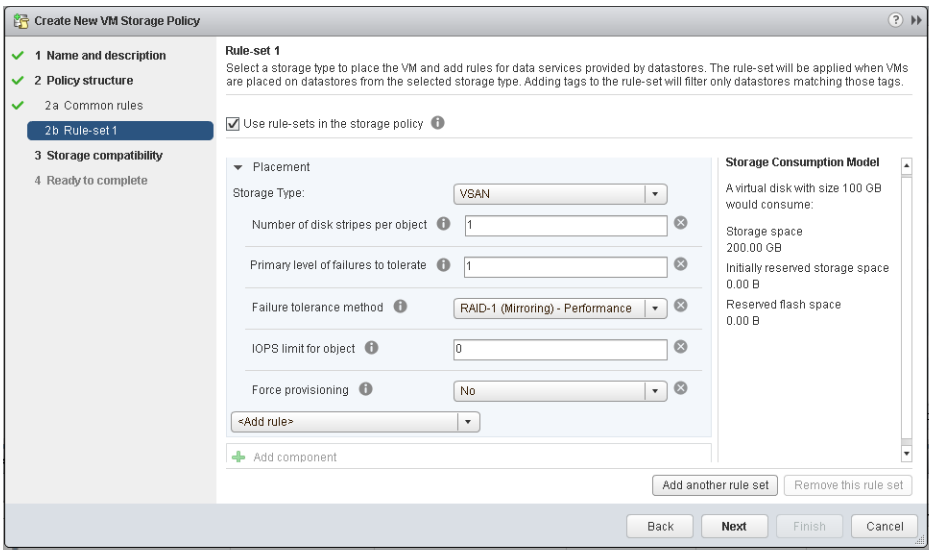
   La directiva de almacenamiento se aplica como la directiva predeterminada al aprovisionar las nuevas máquinas virtuales sin especificar una directiva de almacenamiento de manera explícita para un almacén de datos.

Qué hacer a continuación

Puede definir una nueva directiva de almacenamiento para máquinas virtuales. Consulte "Definir una directiva de almacenamiento de máquinas virtuales para vSAN," página 142.

Definir una directiva de almacenamiento de máquinas virtuales para vSAN

Es posible crear una directiva de almacenamiento en la que se definan los requisitos de almacenamiento para una máquina virtual y sus discos virtuales. En esta directiva, se debe hacer referencia a las funcionalidades de almacenamiento que admite el almacén de datos de vSAN.



Prerequisitos

- Compruebe que el proveedor de almacenamiento de vSAN esté disponible. Consulte "Ver los proveedores de almacenamiento de vSAN," página 139.
- Asegúrese de que estén habilitadas las directivas de almacenamiento para las máquinas virtuales. Para obtener información sobre las directivas de almacenamiento, consulte el documento *Almacenamiento de vSphere*.
- Privilegios requeridos: **Almacenamiento basado en perfiles.Vista de almacenamiento basado en perfiles** y **Almacenamiento basado en perfiles.Actualización de almacenamiento basado en perfiles**

Procedimiento

1. En la página de inicio de vSphere Web Client, haga clic en **Directivas y perfiles** y, a continuación, en **Directivas de almacenamiento de máquina virtual**.
2. Haga clic en el icono **Create a new VM storage policy** (Crear una nueva directiva de almacenamiento de máquina virtual) ( ).
3. En la página de nombre y descripción, seleccione un vCenter Server.
4. Escriba un nombre y una descripción para la directiva de almacenamiento y haga clic en **Next** (Siguiente).
5. En la página de estructura de la directiva, haga clic en **Siguiente**.
6. En la página **Reglas comunes para los servicios de datos proporcionados por los hosts**, haga clic en **Siguiente**.

7 En la página Conjunto de reglas 1, defina el primer conjunto de reglas.

   a Marque la casilla **Usar conjuntos de reglas en la directiva de almacenamiento**.

   b Seleccione **VSAN** en el menú desplegable **Tipo de almacenamiento**.

   La página se ampliará a medida que se agreguen reglas para el almacén de datos de vSAN.

   c Seleccione una regla del menú desplegable **Agregar regla**.

   Asegúrese de proporcionar valores que se ubiquen dentro del rango de valores anunciado por las funcionalidades de almacenamiento del almacén de datos de vSAN.

   Desde el modelo de consumo de almacenamiento, puede consultar el tamaño de disco virtual disponible y los requisitos correspondientes de capacidad y memoria caché, incluido el espacio de almacenamiento reservado que potencialmente podrían consumir las máquinas virtuales al aplicar la directiva de almacenamiento.

   d (Opcional) Agregue funcionalidades basadas en etiquetas.

8 (Opcional) Haga clic en el botón **Agregar otro conjunto de reglas** para agregar otro conjunto de reglas.

9 Haga clic en **Next** (Siguiente).

10 En la página de compatibilidad de almacenamiento, revise la lista de almacenes de datos que coinciden con esta directiva y haga clic en **Siguiente**.

   Para cumplir las condiciones, un almacén de datos no necesita satisfacer todos los conjuntos de reglas incluidos en la directiva. El almacén de datos debe satisfacer al menos uno de los conjuntos de reglas y todas las reglas de dicho conjunto. Verifique que el almacén de datos de vSAN cumpla con los requisitos establecidos en la directiva de almacenamiento y que figure en la lista de almacenes de datos compatibles.

11 En la página de finalización, revise la configuración de la directiva y haga clic en **Finalizar**.

La nueva directiva se agrega a la lista.

Qué hacer a continuación

Asigne esta directiva a una máquina virtual y sus discos virtuales. vSAN coloca los objetos de máquina virtual según los requisitos especificados en la directiva. Para obtener información sobre cómo aplicar directivas de almacenamiento a objetos de máquinas virtuales, consulte el documento *Almacenamiento de vSphere*.

Supervisar vSAN 13

Puede supervisar su entorno de vSAN desde vSphere Web Client.

Puede supervisar todos los objetos en un entorno de vSAN, incluidos los hosts que participan en un clúster de vSAN y el almacén de datos de vSAN. Para obtener más información sobre la supervisión de objetos y recursos de almacenamiento en un clúster de vSAN, consulte el documento *Supervisión y rendimiento de vSphere*.

Este capítulo cubre los siguientes temas:

Supervisar el clúster de vSAN

Puede supervisar el clúster de vSAN y todos los objetos relacionados con él.

Procedimiento

1 Desplácese hasta el clúster de vSAN en vSphere Web Client.

2 Haga clic en la pestaña **Monitor** (Supervisar) y seleccione **vSAN**.

3 Seleccione **Physical Disks** (Discos físicos) para examinar todos los hosts, dispositivos de almacenamiento en caché y dispositivos de capacidad en el clúster.

   vSAN muestra información acerca de los dispositivos de capacidad, como la capacidad total, la capacidad utilizada, la capacidad reservada, el estado de funcionamiento, la ubicación física, etc. La ubicación física se basa en la ubicación de hardware de los dispositivos de memoria caché y de capacidad de los hosts de vSAN.

4 Seleccione un dispositivo de capacidad y haga clic en **Virtual Disks** (Discos virtuales) para consultar las máquinas virtuales que utilizan el dispositivo.

   Puede supervisar diversos aspectos de los objetos de máquinas virtuales, entre ellos, su estado actual y si cumplen con las directivas de almacenamiento asignadas a ellos.

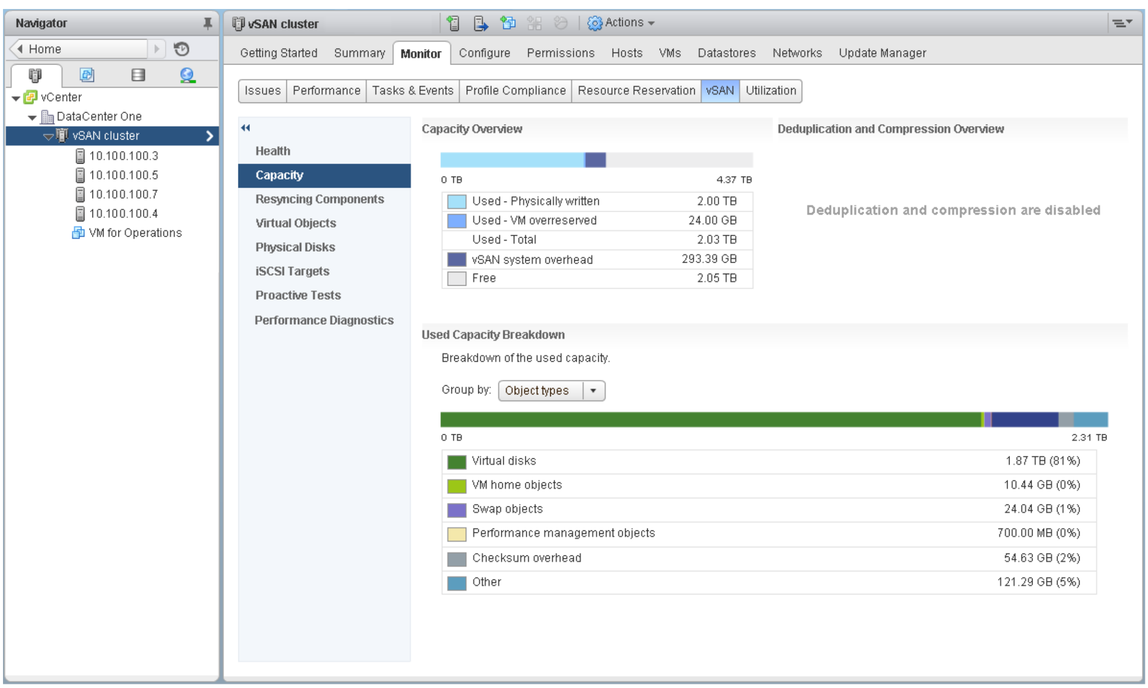
5 Seleccione **Capacity** (Capacidad) para examinar la información sobre la cantidad de capacidad aprovisionada y usada en el clúster, y también para examinar un desglose de la capacidad usada por tipo de objeto o tipo de datos.

6 Seleccione la pestaña **Configurar** y seleccione **General** para comprobar el estado del clúster de vSAN, verificar la conectividad a Internet y examinar el formato en disco utilizado en el clúster.

Supervisar la capacidad de vSAN

Puede supervisar la capacidad del almacén de datos de vSAN, la eficiencia de la desduplicación y compresión, y un desglose del uso de capacidad.

La pestaña Resumen del clúster de vSphere Web Client incluye un resumen de la capacidad de vSAN. También puede visualizar información más detallada en Capacity monitor (Supervisión de capacidad).



Procedimiento

1 Desplácese hasta el clúster de vSAN en vSphere Web Client.

2 Haga clic en la pestaña **Monitor** (Supervisar) y seleccione **vSAN**.

3 Seleccione **Capacidad** para ver la información de capacidad de vSAN.

Información general de capacidad muestra la capacidad de almacenamiento del almacén de datos de vSAN, incluido el espacio usado y el espacio libre. Used Capacity Breakdown (Desglose de capacidad usada) muestra el porcentaje de capacidad usada por los diferentes tipos de objetos o tipos de datos. Si selecciona Tipos de datos, vSAN muestra el porcentaje de capacidad usada por los datos principales de las máquinas virtuales, la sobrecarga de vSAN y la sobrecarga temporal. Si selecciona Tipos de objetos, vSAN muestra el porcentaje de la capacidad usada por los siguientes tipos de objetos:

- Discos virtuales

- Objetos principales de máquinas virtuales
- Objetos de intercambio
- Objetos de administración de rendimiento
- Archivos .vmem
- Sobrecarga de suma de comprobación
- Memoria de instantáneas
- Sobrecarga de desduplicación y compresión
- Espacio según consideración del motor de desduplicación
- Objetos de inicio y de destino iSCSI y LUN de iSCSI
- Otros tipos de objetos, como archivos creados por el usuario, plantillas de máquinas virtuales, etc.

Si habilita la desduplicación y la compresión en el clúster, Deduplication and Compression Overview (Descripción general de desduplicación y compresión) muestra la información de capacidad relacionada con dicha característica. Cuando se habilita la desduplicación y la compresión, es posible que las actualizaciones de capacidad demoren varios minutos en aparecer en Capacity monitor (Supervisión de capacidad), a medida que se va recuperando y reasignando el espacio en disco. Para obtener más información sobre la desduplicación y compresión, consulte "Uso de la desduplicación y compresión," página 75.

Supervisar dispositivos virtuales en el clúster de vSAN

Puede ver el estado de los discos virtuales en el clúster de vSAN.

Cuando uno o más hosts no pueden comunicarse con el almacén de datos de vSAN, no se muestra la información sobre los dispositivos virtuales.

Procedimiento

1. Desplácese hasta el clúster de vSAN en vSphere Web Client.
2. Haga clic en la pestaña **Monitor** (Supervisar) y seleccione **vSAN**.
3. Seleccione **Discos virtuales** para ver todos los hosts y los discos virtuales correspondientes del clúster de vSAN, incluidos los hosts y los dispositivos de memoria caché y de capacidad que sus componentes consumen actualmente.
4. Seleccione la carpeta del **directorio principal de la máquina virtual** y haga clic en la pestaña **Physical Disk Placement** (Ubicación de discos físicos) para ver la información de los dispositivos, como el nombre, el identificador o el UUID, etc.

   Haga clic en la pestaña **Compliance Failures** (Errores de cumplimiento) para comprobar el estado de cumplimiento de la máquina virtual.
5. Seleccione el **disco duro** en una de las máquinas virtuales y haga clic en la pestaña **Physical Disk Placement** (Ubicación de discos físicos) para ver la información del dispositivo, como el nombre, el identificador o el UUID, la cantidad de dispositivos que se usan para cada máquina virtual y la manera en que se reflejan en los distintos hosts.

   Haga clic en la pestaña **Compliance Failures** (Errores de cumplimiento) para comprobar el estado de cumplimiento del dispositivo virtual.
6. Haga clic en la pestaña **Compliance Failures** (Errores de cumplimiento) para comprobar el estado de cumplimiento de las máquinas virtuales.

Acerca de la resincronización del clúster de vSAN

Puede supervisar el estado de los objetos de máquinas virtuales que se van a resincronizar en el clúster de vSAN.

Cuando se produce un error en un dispositivo de hardware, un host o una red, o si un host se pone en modo de mantenimiento, vSAN inicia la resincronización en el clúster de vSAN. Sin embargo, antes de iniciar las tareas de resincronización, es posible que vSAN espere un momento hasta que los componentes con errores vuelvan a conectarse.

Los siguientes eventos activan la resincronización en el clúster:

- Editar la directiva de almacenamiento de una máquina virtual (VM). Cuando se modifica la configuración de la directiva de almacenamiento de máquina virtual, es posible que vSAN inicie la recreación de objetos y la resincronización posterior de los objetos.

  Algunos cambios de directivas podrían hacer que vSAN cree otra versión de un objeto y la sincronice con la versión anterior. Una vez finalizada la sincronización, se descarta el objeto original.

  vSAN garantiza que las máquinas virtuales sigan en ejecución y que no se vean interrumpidas por este proceso. Este proceso podría requerir una capacidad adicional temporal.

- Reiniciar un host después de un error.
- Recuperar hosts de un error permanente o a largo plazo. Si un host no está disponible durante más de 60 minutos (valor predeterminado), vSAN crea copias de datos para recuperar el cumplimiento completo de las directivas.
- Evacuar datos utilizando el modo de migración de datos completa antes de poner un host en modo de mantenimiento.
- Superar el umbral de uso de un dispositivo de capacidad. La resincronización se activa cuando el uso del dispositivo de capacidad en el clúster de vSAN alcanza o excede el nivel de umbral de 80 %.

Si una máquina virtual no responde debido a la latencia que la resincronización genera, se puede regular el valor de E/S por segundo utilizado para la resincronización.

Supervisar las tareas de resincronización en el clúster de vSAN

Para evaluar el estado de los objetos que se van a volver a sincronizar, puede supervisar las tareas de resincronización que están en curso.

Prerequisitos

Verifique que los hosts del clúster de vSAN ejecuten ESXi 6.5 o versiones posteriores.

Procedimiento

1. Desplácese hasta el clúster de vSAN en vSphere Web Client.
2. Seleccione la pestaña **Monitor** (Supervisar) y haga clic en **vSAN**.
3. Seleccione **Resyncing Components** (Resincronización de componentes) para hacer un seguimiento del progreso de la resincronización de los objetos de máquina virtual y la cantidad de bytes restantes antes de que finalice la resincronización.

   También puede ver información sobre la cantidad de objetos que se están sincronizando actualmente en el clúster, el tiempo estimado para que finalice la resincronización, el tiempo restante para que los objetos de almacenamiento cumplan por completo la directiva de almacenamiento asignada, etc.

   Si el clúster tiene problemas de conectividad, es posible que los datos de la página Resyncing Components (Resincronización de componentes) no se actualicen según lo previsto y que los campos reflejen información incorrecta.

Regular la actividad de resincronización en el clúster de vSAN

Es posible reducir el número de E/S por segundo que se usan para ejecutar tareas de resincronización en los grupos de discos del clúster de vSAN. La regulación de la resincronización es una configuración para todo el clúster y se aplica en cada grupo de discos.

Si las máquinas virtuales no responden a la latencia provocada por la resincronización, se puede regular el número de E/S por segundo utilizado para la resincronización. Tenga en cuenta la regulación de la resincronización solo si esta produce latencias en el clúster o si el tráfico de resincronización en un host es demasiado alto.

La regulación de la resincronización puede incrementar el tiempo requerido para completar la resincronización. La reprotección de las máquinas virtuales que no cumplen con las normas puede retrasarse.

Procedimiento

1 Desplácese hasta el clúster de vSAN en vSphere Web Client.

2 Seleccione la pestaña **Monitor** (Supervisar) y haga clic en **vSAN**.

3 Seleccione **Resyncing Components** (Resincronización de componentes) y haga clic en **Resync Throttling** (Regulación de la resincronización).

4 (Opcional) Haga clic en **Show current resync traffic per host** (Mostrar tráfico de resincronización actual por host) para ver la actividad de resincronización.

5 Marque la casilla **Enable throttling for resyncing components traffic** (Habilitar regulación del tráfico de resincronización de componentes).

6 Mueva el control deslizante para establecer la regulación del siguiente modo:

- Mueva el control deslizante hacia la derecha para incrementar la cantidad permitida de E/S por segundo para la resincronización.
- Mueva el control deslizante hacia la izquierda para reducir la cantidad permitida de E/S por segundo para la resincronización.

Como regla general, se regula la cantidad de E/S por segundo a la mitad y se permite cierto tiempo para que el clúster se adapte. Si se requieren más acciones, vuelva a regular la cantidad de E/S por segundo a la mitad hasta que el clúster se estabilice.

7 Haga clic en **OK** (Aceptar).

Supervisar dispositivos que participan en almacenes de datos de vSAN

Compruebe el estado de los dispositivos que crean copias de seguridad del almacén de datos de vSAN. Puede comprobar si los dispositivos experimentan problemas.

Procedimiento

1 Desplácese hasta Storage (Almacenamiento) en vSphere Web Client.

2 Seleccione el almacén de datos de vSAN.

3 Haga clic en la pestaña **Configurar**.

Puede visualizar información general sobre el almacén de datos de vSAN, incluida la capacidad, las funcionalidades y la directiva de almacenamiento predeterminada.

4 Haga clic en **Device Backing** (Respaldo de dispositivo) y seleccione el grupo de discos para mostrar los dispositivos locales en la tabla Disks (Discos) ubicada en la parte inferior de la página.

5 Para mostrar columnas que no están visibles, haga clic con el botón derecho en el encabezado de la columna y seleccione **Show/Hide Columns** (Mostrar/ocultar columnas).

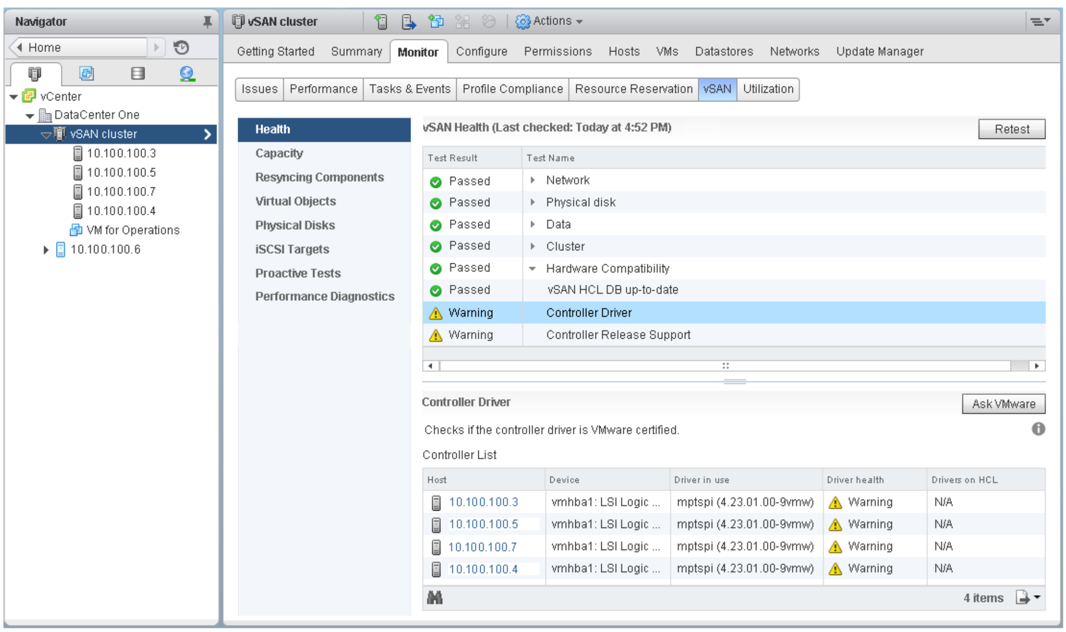
6 Seleccione las columnas que desea mostrar y haga clic en **OK** (Aceptar).

Las columnas seleccionadas se muestran en la tabla Disks (Dispositivos).

Supervisar el estado de vSAN

Puede comprobar el estado del clúster de vSAN.

Puede utilizar las comprobaciones de estado de vSAN para supervisar el estado de los componentes del clúster, diagnosticar problemas y resolverlos. Las comprobaciones de estado abarcan la compatibilidad del hardware, la configuración y el funcionamiento de la red, las opciones de configuración avanzadas de vSAN, el estado de los dispositivos de almacenamiento y los objetos de las máquinas virtuales.



Las comprobaciones de estado de vSAN se dividen en categorías. Cada categoría contiene comprobaciones de estado individuales.

Tabla 13-1. Categorías de comprobación de estado de vSAN

Categoría de comprobación de estado	Descripción
Hardware Compatibility (Compatibilidad de hardware)	Permite supervisar los componentes del clúster y garantizar que utilizan hardware, software y controladores admitidos.
Performance Service (Servicio de rendimiento)	Permite supervisar el estado del servicio de rendimiento de vSAN.
Network (Red)	Permite supervisar el estado de la red de vSAN.
Physical disk (Disco físico)	Permite supervisar el estado de los dispositivos físicos en el clúster de vSAN.
Data (Datos)	Permite supervisar el estado de los datos de vSAN.
Cluster (Clúster)	Permite supervisar el estado del clúster de vSAN.
Limits (Límites)	Permite supervisar los límites del clúster de vSAN.
Estado en línea	Permite supervisar el estado del clúster de vSAN y enviarlo al sistema de back-end de análisis VMware para un análisis avanzado. Debe participar en el programa de mejora de la experiencia de cliente para poder realizar comprobaciones de estado en línea.

Tabla 13-1. Categorías de comprobación de estado de vSAN (Continua)

Categoría de comprobación de estado	Descripción
Servicio del destino iSCSI de vSAN	Permite supervisar el servicio del destino iSCSI, incluidos la configuración de red y el estado en tiempo de ejecución.
Cifrado	Permite supervisar el estado de cifrado de vSAN.
Clúster ampliado	Permite supervisar el estado del clúster ampliado, si corresponde.

vSAN vuelve a probar periódicamente cada comprobación de estado y actualiza los resultados. Para ejecutar las comprobaciones de estado y actualizar los resultados de inmediato, haga clic en el botón **Retest** (Volver a probar).

Si participa en el programa de mejora de la experiencia de cliente, puede ejecutar las comprobaciones de estado y enviar los datos a VMware para un análisis avanzado. Haga clic en el botón **Retest with Online health** (Volver a probar con el estado en línea).

Para obtener más información sobre las comprobaciones de estado de vSAN, consulte *Guía de complementos de comprobación de estado de VMware Virtual SAN*.

Supervisar el estado de vSAN en un host

El cliente host ESXi es una interfaz basada en navegador para la administración de un único host ESXi. Permite administrar el host cuando vCenter Server no está disponible. El cliente host incluye pestañas para administrar y supervisar vSAN en el nivel del host.

- La pestaña **vSAN** muestra la configuración básica de vSAN.
- En la pestaña **Hosts**, se pueden ver los hosts que participan en el clúster de vSAN.
- En la pestaña **Health** (Estado), se pueden ver las comprobaciones de estado en el nivel del host.

Configurar vSAN Health Service

Puede configurar el intervalo de comprobación de estado de vSAN Health Service.

vSAN Health Service está activado de forma predeterminada. Puede activar o desactivar las comprobaciones periódicas de estado y establecer el intervalo de comprobación de estado.

Procedimiento

1. Desplácese hasta el clúster de vSAN en vSphere Web Client.
2. Haga clic en la pestaña **Configurar**.
3. En vSAN, seleccione **Health and Performance** (Estado y rendimiento).
4. Haga clic en el botón **Editar configuración** de los servicios de estado.
    a. Para desactivar las comprobaciones periódicas de estado, anule la selección de **Turn ON periodical health check** (Activar comprobación periódica de estado).

       También puede establecer el intervalo entre las comprobaciones de estado.
    b. Para activar las comprobaciones periódicas de estado, seleccione **Turn ON periodical health check** (Activar comprobación periódica de estado).

Comprobar el estado de vSAN

Puede visualizar el estado de las comprobaciones de estado de vSAN para verificar la configuración y el funcionamiento del clúster de vSAN.

Prerequisitos

vSAN Health Service debe activarse antes de que pueda visualizar las comprobaciones de estado.

Procedimiento

1. Desplácese hasta el clúster de vSAN en vSphere Web Client.
2. Haga clic en la pestaña **Monitor** (Supervisar) y seleccione **vSAN**.
3. Seleccione **Estado** para examinar las categorías de comprobación del estado de vSAN.

   Si la columna Test Result (Resultado de la prueba) muestra Warning (Advertencia) o Failed (Error), expanda la categoría para examinar los resultados de las comprobaciones de estado individuales.
4. Seleccione una comprobación de estado individual y examine la información detallada en la parte inferior de la página.

   Puede hacer clic en el botón **Ask VMware** (Preguntar a VMware) para abrir un artículo de la base de conocimiento que describe la comprobación de estado y proporciona información sobre cómo resolver el problema.

Supervisar vSAN desde el cliente del host ESXi

Puede supervisar el estado de vSAN y la configuración básica a través del cliente host ESXi.

Prerequisitos

vSAN Health Service debe activarse antes de que pueda visualizar las comprobaciones de estado.

Procedimiento

1. Abra un navegador y escriba la dirección IP del host.

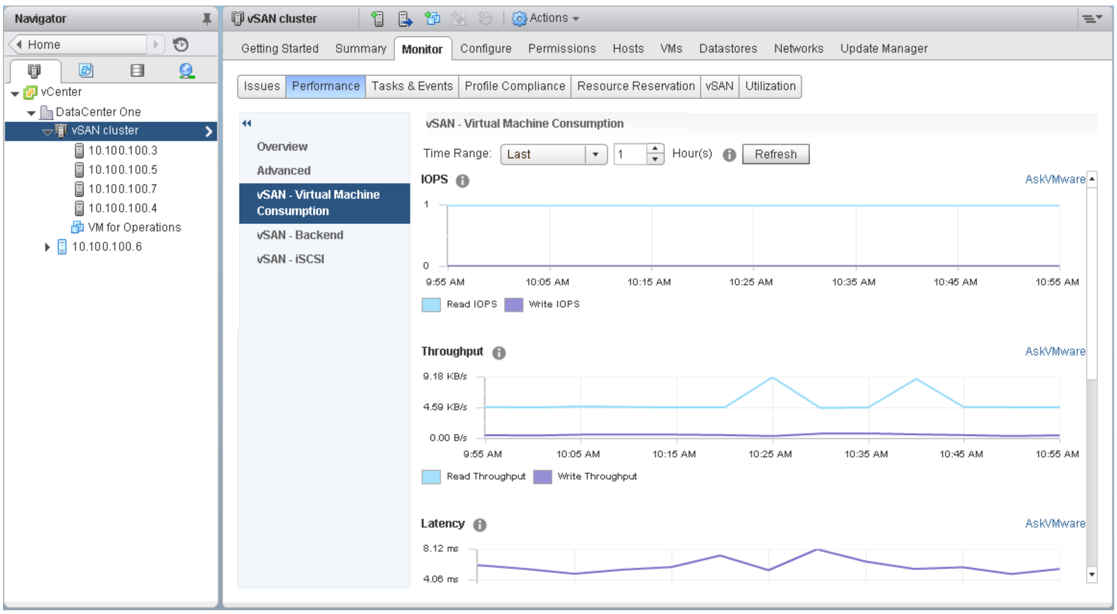
   El navegador lo redirigirá a la página de inicio de sesión del cliente host.
2. Escriba el nombre de usuario y la contraseña del host, y haga clic en **Login** (Iniciar sesión).
3. En el navegador del cliente host, haga clic en **Storage** (Almacenamiento).
4. En la página principal, haga clic en el almacén de datos de vSAN para mostrar el vínculo Monitor (Supervisar) en el navegador.
5. Haga clic en las pestañas para ver la información de vSAN del host.
   a. Haga clic en la pestaña **vSAN** para mostrar la configuración básica de vSAN.
   b. Haga clic en la pestaña **Hosts** para ver los hosts que participan en el clúster de vSAN.
   c. Haga clic en la pestaña **Health** (Estado) para mostrar las comprobaciones de estado en el nivel del host.
6. (Opcional) En la pestaña **vSAN**, haga clic en **Edit Settings** (Editar configuración) para solucionar los problemas de configuración en el nivel del host. Seleccione los valores que coincidan con la configuración del clúster de vSAN.

   Seleccione los valores que coincidan con la configuración del clúster de vSAN y haga clic en **Guardar**.

Supervisar el rendimiento de vSAN

Puede utilizar el servicio de rendimiento de vSAN para supervisar el rendimiento de su entorno de vSAN e investigar potenciales problemas.

El servicio de rendimiento recopila y analiza estadísticas de rendimiento y muestra los datos en formato de gráfico. Se pueden utilizar los gráficos de rendimiento para administrar la carga de trabajo y determinar la causa principal de determinados problemas.



Cuando se activa el servicio de rendimiento de vSAN, el resumen del clúster muestra una descripción general de las estadísticas de rendimiento de vSAN, incluidas las E/S por segundo, el rendimiento y la latencia. Puede visualizar estadísticas de rendimiento detalladas para el clúster y para cada host, grupo de discos y disco del clúster de vSAN. También puede visualizar las tablas de rendimiento para las máquinas virtuales y los discos virtuales.

Activar el servicio de rendimiento de vSAN

Cuando crea un clúster de vSAN, el servicio de rendimiento se encuentra deshabilitado. Active el servicio de rendimiento de vSAN para supervisar el rendimiento de los clústeres, los hosts, los discos y las máquinas virtuales de vSAN.

Cuando active el servicio de rendimiento, vSAN colocará un objeto de la base de datos Stats en el almacén de datos para recolectar los datos estadísticos. La base de datos Stats es un objeto de espacio de nombres en el almacén de datos de vSAN del clúster.

Prerequisitos

- Todos los hosts del clúster de vSAN deben ejecutar ESXi 6.5 o una versión posterior.
- Antes de habilitar el servicio de rendimiento de vSAN, asegúrese de que el clúster esté configurado correctamente y no existan problemas de estado sin resolver.

Procedimiento

1 Desplácese hasta el clúster de vSAN en el navegador de vSphere Web Client.

2 Haga clic en la pestaña **Configurar**.

3 En vSAN, seleccione **Estado y rendimiento**.

4 Haga clic en **Editar** para editar los ajustes del servicio de rendimiento.

5 Marque la casilla **Turn On vSAN performance service** (Activar servicio de rendimiento de vSAN).

Puede desactivar el servicio de rendimiento de vSAN anulando la selección de la casilla.

6 Seleccione una directiva de almacenamiento para el objeto de la base de datos Stats y haga clic en **OK** (Aceptar).

Usar el intervalo de tiempo guardado

Puede seleccionar intervalos de tiempo guardados desde el selector correspondiente en las vistas de rendimiento.

Puede guardar manualmente un intervalo de tiempo con un nombre personalizado. Cuando ejecuta una prueba de rendimiento de almacenamiento, el intervalo de tiempo seleccionado se guarda automáticamente. Puede guardar un intervalo de tiempo para cualquiera de las vistas de rendimiento.

Prerequisitos

- El servicio de rendimiento de vSAN debe activarse.
- Todos los hosts del clúster de vSAN deben ejecutar ESXi 6.6 o una versión posterior.

Procedimiento

1 Desplácese hasta el clúster de vSAN en el navegador de vSphere Web Client.

2 Haga clic en la pestaña **Monitor** (Supervisar) y haga clic en **Performance** (Rendimiento).

3 Seleccione cualquier pestaña, como **vSAN - Backend** (vSAN: back-end). En el menú desplegable de intervalo de tiempo, seleccione **Save time range...** (Guardar intervalo de tiempo...).

4 Escriba un nombre para el intervalo de tiempo seleccionado.

5 Haga clic en **OK** (Aceptar).

Ver el rendimiento del clúster de vSAN

Puede utilizar las tablas de rendimiento del clúster de vSAN para supervisar la carga de trabajo del clúster y determinar la causa raíz de los problemas.

Cuando se activa el servicio de rendimiento, el resumen del clúster muestra una descripción general de las estadísticas de rendimiento de vSAN, incluidas las E/S por segundo, el rendimiento y la latencia de vSAN. A nivel del clúster, puede visualizar tablas estadísticas detalladas para el consumo de máquinas virtuales y extremo posterior de vSAN.

Prerequisitos

El servicio de rendimiento de vSAN debe activarse antes de que pueda visualizar las tablas de rendimiento.

Procedimiento

1 Desplácese hasta el clúster de vSAN en el navegador de vSphere Web Client.

2 Haga clic en la pestaña **Monitor** (Supervisar) y haga clic en **Performance** (Rendimiento).

3 Seleccione **vSAN - Virtual Machine Consumption** (vSAN: consumo de máquina virtual). Seleccione un intervalo de tiempo para la consulta.

vSAN muestra tablas de rendimiento para los clientes que se ejecutan en el clúster, incluidas las E/S por segundo, el rendimiento, la latencia, las congestiones y las E/S pendientes. Las estadísticas de estas tablas se incorporan a partir de los hosts dentro del clúster.

4 Seleccione **vSAN - Backend** (vSAN: back-end). Seleccione un intervalo de tiempo para la consulta.

vSAN muestra tablas de rendimiento para las operaciones de back-end del clúster, incluidas las E/S por segundo, el rendimiento, la latencia, las congestiones y las E/S pendientes. Las estadísticas de estas tablas se incorporan a partir de los hosts dentro del clúster.

5 Seleccione **vSAN - iSCSI** (vSAN: iSCSI) y un destino iSCSI o un LUN. Seleccione un intervalo de tiempo para la consulta.

NOTA: Para ver las tablas de rendimiento de iSCSI, todos los hosts del clúster de vSAN deben ejecutar ESXi 6.6 o una versión posterior.

vSAN muestra tablas de rendimiento para los destinos iSCSI o LUN, incluidas las E/S por segundo, el ancho de banda, la latencia y las E/S pendientes.

Ver el rendimiento del host de vSAN

Puede utilizar las tablas de rendimiento del host de vSAN para supervisar la carga de trabajo de los hosts y determinar la causa raíz de los problemas. Puede visualizar tablas de rendimiento de vSAN para los hosts, grupos de discos y dispositivos de almacenamiento individuales.

Cuando se activa el servicio de rendimiento, el resumen del host muestra estadísticas de rendimiento para cada host y sus discos asociados. A nivel del host, puede visualizar tablas estadísticas detalladas para el consumo de máquinas virtuales y extremo posterior de vSAN, incluidas las E/S por segundo, el rendimiento, la latencia y la congestión. Hay gráficos adicionales disponibles para ver la tasa de aciertos y la de E/S por segundo de lectura de memoria caché del cliente local. A nivel del grupo de discos, puede visualizar estadísticas para el grupo de discos. A nivel de disco, puede visualizar estadísticas para un dispositivo de almacenamiento individual.

Prerequisitos

El servicio de rendimiento de vSAN debe activarse antes de que pueda visualizar las tablas de rendimiento.

Para ver las tablas de rendimiento siguientes, los hosts del clúster de vSAN deben ejecutar ESXi 6.6 o una versión posterior: adaptadores físicos, adaptadores de VMkernel, agregación de adaptadores de VMkernel, iSCSI, E/S de resincronización de vSAN: back-end, E/S por segundo de resincronización, capacidad de proceso de resincronización, latencia de resincronización de grupo de discos.

Procedimiento

1 Desplácese hasta el clúster de vSAN en el navegador de vSphere Web Client y seleccione un host.

2 Haga clic en la pestaña **Monitor** (Supervisar) y haga clic en **Performance** (Rendimiento).

3 Seleccione **vSAN - Virtual Machine Consumption** (vSAN: consumo de máquina virtual). Seleccione un intervalo de tiempo para la consulta.

vSAN muestra tablas de rendimiento para los clientes que se ejecutan en el host, incluidas las E/S por segundo, el rendimiento, la latencia, las congestiones y las E/S pendientes.

4 Seleccione **vSAN - Backend** (vSAN: back-end). Seleccione un intervalo de tiempo para la consulta.

vSAN muestra tablas de rendimiento para las operaciones de back-end del host, incluidas las E/S por segundo, la capacidad de proceso, la latencia, las congestiones, las E/S pendientes y las E/S de resincronización.

5 Seleccione **vSAN - Disk Group** (Virtual SAN: grupo de discos) y seleccione un grupo de discos. Seleccione un intervalo de tiempo para la consulta.

   vSAN muestra tablas de rendimiento para el grupo de discos, incluidas las E/S por segundo del extremo frontal (invitado), el rendimiento y la latencia, así como las E/S por segundo y la latencia de sobrecarga. También muestra la proporción de aciertos de almacenamiento en caché de lectura, las expulsiones, el porcentaje libre de búfer de escritura, la capacidad y el uso, la proporción de descarga del disco de almacenamiento en caché, las congestiones, las E/S pendientes, el tamaño de las E/S pendientes, el porcentaje de E/S retrasadas, la latencia promedio de las E/S retrasadas, las E/S por segundo de la cola interna, las E/S por segundo de resincronización, la capacidad de proceso de resincronización y la latencia de resincronización.

6 Seleccione **vSAN - Disk** (vSAN: disco) y seleccione un disco. Seleccione un intervalo de tiempo para la consulta.

   vSAN muestra tablas de rendimiento para el disco, incluidas las E/S por segundo de la capa física/firmware, el rendimiento y la latencia.

7 Seleccione **vSAN - Physical Adapters** (vSAN: adaptadores físicos) y seleccione una NIC. Seleccione un intervalo de tiempo para la consulta.

   vSAN muestra tablas de rendimiento para la NIC física (physical NIC, pNIC), que incluyen la capacidad de proceso, los paquetes por segundo y la proporción de pérdida de paquetes.

8 Seleccione **vSAN - VMkernel Adapters** (vSAN: adaptadores de VMkernel) y seleccione un adaptador de VMkernel, como vmk1. Seleccione un intervalo de tiempo para la consulta.

   vSAN muestra tablas de rendimiento para el adaptador de VMkernel, que incluyen la capacidad de proceso, los paquetes por segundo y la proporción de pérdida de paquetes.

9 Seleccione **vSAN - VMkernel Adapters Aggregation** (vSAN: agregación de adaptadores de VMkernel). Seleccione un intervalo de tiempo para la consulta.

   vSAN muestra tablas de rendimiento para todas las E/S de red procesadas en los adaptadores de red utilizados por vSAN, que incluyen la capacidad de proceso, los paquetes por segundo y la proporción de pérdida de paquetes.

10 Seleccione **vSAN - iSCSI** (vSAN: iSCSI). Seleccione un intervalo de tiempo para la consulta.

   vSAN muestra tablas de rendimiento para todos los servicios iSCSI del host, que incluyen las E/S por segundo, el ancho de banda, la latencia y las E/S pendientes.

Ver el rendimiento de las máquinas virtuales en vSAN

Puede utilizar las tablas de rendimiento de la máquina virtual de vSAN para supervisar la carga de trabajo de sus máquinas virtuales y discos virtuales.

Cuando active el servicio de rendimiento, puede ver tablas estadísticas detalladas para el rendimiento de la máquina virtual y el rendimiento del disco virtual. Las estadísticas de rendimiento de la máquina virtual no pueden recolectarse durante la migración entre los hosts. Por lo tanto, es posible que observe una brecha de varios minutos en la tabla de rendimiento de la máquina virtual.

NOTA: El servicio de rendimiento solo admite controladoras SCSI virtuales para discos virtuales. No se admiten discos virtuales que utilicen otras controladoras, como IDE.

Prerequisitos

El servicio de rendimiento de vSAN debe activarse antes de que pueda visualizar las tablas de rendimiento.

Procedimiento

1 Desplácese hasta el clúster de vSAN en el navegador de vSphere Web Client y seleccione una máquina virtual.

2 Haga clic en la pestaña **Monitor** (Supervisar) y haga clic en **Performance** (Rendimiento).

3 Seleccione **vSAN - Virtual Machine Consumption** (vSAN: consumo de máquina virtual). Seleccione un intervalo de tiempo para la consulta.

   vSAN muestra tablas de rendimiento para la máquina virtual, incluidas las E/S por segundo, el rendimiento y la latencia.

4 Seleccione **vSAN - Virtual Disk** (vSAN: disco virtual). Seleccione un intervalo de tiempo para la consulta.

   vSAN muestra las tablas de rendimiento para los discos virtuales, incluidas las E/S por segundo, las E/S por segundo normalizadas y retrasadas, las E/S por segundo de SCSI virtual, el rendimiento de SCSI virtual y la latencia de SCSI virtual.

Usar diagnósticos de rendimiento de vSAN

Puede usar los diagnósticos de rendimiento de vSAN para mejorar el rendimiento del clúster de vSAN y solucionar problemas de rendimiento.

La herramienta de diagnósticos de rendimiento de vSAN analiza los bancos de pruebas ejecutados previamente que se recopilaron a partir del servicio de rendimiento de vSAN. Puede detectar problemas, sugerir pasos de solución y proporcionar gráficos de rendimiento de respaldo para ofrecer más detalles.

El servicio de rendimiento de vSAN proporciona los datos que se utilizan para analizar los diagnósticos de rendimiento de vSAN. vSAN utiliza CEIP para enviar datos a VMware y analizarlos.

NOTA: No utilice los diagnósticos de rendimiento de vSAN para evaluar de forma general el rendimiento en un clúster de vSAN de producción.

Prerequisitos

- El servicio de rendimiento de vSAN debe activarse.
- vCenter Server requiere acceso a Internet para descargar las revisiones y las imágenes ISO.
- Debe participar en el programa de mejora de la experiencia de cliente (Customer Experience Improvement Program, CEIP).

Procedimiento

1 Desplácese hasta el clúster de vSAN en el navegador de vSphere Web Client.

2 Haga clic en la pestaña **Monitor** (Supervisar) y seleccione **vSAN**.

3 Seleccione **Diagnósticos de rendimiento**.

4 Seleccione un objetivo de banco de pruebas del menú desplegable.

   Puede seleccionar un objetivo en función de la mejora del rendimiento que desee alcanzar, como E/S por segundo máximas, capacidad de proceso máxima o latencia mínima.

5 Seleccione un intervalo de tiempo para la consulta.

   El intervalo de tiempo predeterminado es la hora más reciente. Puede aumentar el intervalo para incluir las últimas 24 horas, o definir un intervalo de tiempo personalizado dentro de los últimos 90 días. Si utilizó la herramienta HCIbench para ejecutar pruebas de banco de pruebas de rendimiento en el clúster de vSAN, los intervalos de tiempo de esas pruebas aparecerán en el menú desplegable.

6 Haga clic en **Enviar**.

Al hacer clic en **Enviar**, vSAN transmite los datos de rendimiento al servidor de análisis de back-end de vSphere. Después de analizar los datos, la herramienta de diagnósticos de rendimiento de vSAN muestra una lista de los problemas que podrían haber afectado al rendimiento de banco de pruebas del objetivo seleccionado.

Puede hacer clic para expandir cada problema y ver más detalles acerca de cada uno de ellos, como una lista de elementos afectados. También puede hacer clic en el vínculo **AskVMware** para mostrar un artículo de la base de conocimientos que describe las recomendaciones para solucionar el problema y lograr sus objetivos de rendimiento.

Acerca de la redistribución del clúster de vSAN

Cuando cualquier dispositivo de capacidad del clúster alcanza un uso del 80 %, vSAN reequilibra automáticamente el clúster hasta que el uso de todos los dispositivos de capacidad se encuentre por debajo del umbral.

El reequilibrio del clúster distribuye de forma uniforme los recursos en este para mantener niveles coherentes de rendimiento y disponibilidad del clúster.

Otras operaciones que pueden iniciar el reequilibrio del clúster:

- Si vSAN detecta errores de hardware en el clúster
- Si los hosts de vSAN se colocan en el modo de mantenimiento con la opción **Evacuar todos los datos**
- Si los hosts de vSAN se colocan en el modo de mantenimiento con **Garantizar accesibilidad a los datos** cuando los objetos con la asignación PFTT=0 residen en el host.

NOTA: A fin de proporcionar espacio suficiente para el mantenimiento y la reprotección, y de minimizar los eventos de reequilibrio automático en el clúster de vSAN, considere la posibilidad de mantener un 30 % de capacidad disponible en todo momento.

Puede volver a equilibrar manualmente el clúster de vSAN a través de Ruby vSphere Console (RVC). Consulte "Redistribuir de forma manual," página 159.

Redistribución automática

De forma predeterminada, vSAN redistribuye automáticamente el clúster de vSAN cuando un dispositivo de capacidad alcanza un uso del 80 %. La redistribución también se realiza cuando coloca un host de vSAN en el modo de mantenimiento.

Ejecute los siguientes comandos de RVC para supervisar la operación de redistribución en el clúster:

- `vsan.check_limits`. Comprueba si la utilización del espacio en disco está equilibrada en el clúster.
- `vsan.whatif_host_failures`. Analiza la utilización de capacidad actual por host, interpreta si un solo error de host puede obligar al clúster a agotar el espacio para reprotección y analiza de qué manera un error de host puede afectar la capacidad del clúster, la reserva de memoria caché y los componentes del clúster.

  El uso de la capacidad física que se muestra como la salida del comando corresponde al uso promedio de todos los dispositivos del clúster de vSAN.
- `vsan.resync_dashboard`. Supervisa todas las tareas de reconstrucción en el clúster.

Para obtener información sobre las opciones de los comandos de RVC, consulte la *Guía de referencia de los comandos de RVC*.

Redistribuir de forma manual

Puede redistribuir de forma manual a través de la comprobación de estado del clúster o mediante el uso de los comandos de RVC.

Si la comprobación de estado de equilibrio de discos de vSAN tiene un error, puede iniciar una redistribución manual en vSphere Web Client. En Cluster health (Estado de clúster), acceda a vSAN Disk Balance health check (Comprobación de estado de equilibrio de discos de vSAN) y haga clic en el botón **Rebalance Disks** (Volver a equilibrar discos).

Utilice los siguientes comandos de RVC para redistribuir de forma manual el clúster:

- `vsan.check_limits`. Compruebe si algún dispositivo de capacidad en el clúster de vSAN se está aproximando al límite del umbral del 80 %.
- `vsan.proactive_rebalance [opts]<Path to ClusterComputeResource> --start`. Inicia manualmente la operación de redistribución. Cuando se ejecuta el comando, vSAN examina el clúster para buscar la distribución actual de los componentes y comienza a equilibrar la distribución de los componentes en el clúster. Use las opciones de los comandos para especificar durante cuánto tiempo desea ejecutar la operación de redistribución en el clúster y cuántos datos por hora desea transferir para cada host de vSAN. Para obtener información sobre las opciones de los comandos para la administración de la operación de redistribución en el clúster de vSAN, consulte la *guía de referencia de los comandos de RVC*.

  Debido a que la redistribución del clúster genera operaciones de E/S sustanciales, puede ser lenta y puede afectar el rendimiento de las máquinas virtuales.

NOTA: Cuando se vuelven a equilibrar los discos manualmente, la operación se ejecuta durante el periodo seleccionado aunque no se tengan que mover más datos. El periodo predeterminado es de 24 horas. Si no se mueve ningún dato, vSAN finaliza la tarea de reequilibrio.

Puede configurar una alarma que le notifique cuando el espacio aprovisionado alcance un umbral determinado. Consulte "Crear una alarma de vCenter Server para un evento de vSAN," página 162.

Equilibrar el uso de disco en el clúster de vSAN

Cuando un clúster de vSAN se desequilibra, puede volver a equilibrar el uso del disco.

Si elimina dispositivos de capacidad del clúster de vSAN y agrega otros nuevos, el clúster de vSAN podría desequilibrarse desde una perspectiva de uso de la capacidad. Después de que la supervisión del estado de vSAN le advierta de que existen desequilibrios, podrá volver a equilibrar el clúster.

Prerequisitos

Realice la operación de nuevo equilibrado fuera de las horas de producción para evitar que repercuta en exceso en el clúster.

Procedimiento

1. Desplácese hasta el clúster de vSAN en vSphere Web Client.
2. Haga clic en la pestaña **Monitor** (Supervisar) y seleccione **vSAN**.
3. Haga clic en **Health** (Estado).
4. En la tabla de vSAN Health Service, seleccione **Advertencia: Equilibro de disco de vSAN**.

   Puede revisar el equilibrio de disco de los hosts.
5. Haga clic en el botón **Rebalance Disks** (Volver a equilibrar discos) para volver a equilibrar su clúster.

En esta operación, algunos componentes se moverán de los discos sobreutilizados a los discos infrautilizados.

Usar las alarmas predeterminada de vSAN

Es posible usar las alarmas predeterminadas de vSAN para supervisar los clústeres, los hosts y las licencias de vSAN existentes.

Las alarmas predeterminadas se activan de manera automática cuando los eventos que corresponden a las alarmas se activan o si se cumplen una o varias de las condiciones especificadas en las alarmas. No es posible editar las condiciones ni eliminar las alarmas predeterminadas. Para configurar alarmas específicas para sus requisitos, debe crear alarmas personalizadas para vSAN. Consulte "Crear una alarma de vCenter Server para un evento de vSAN," página 162.

La tabla enumera las alarmas predeterminadas de vSAN.

Tabla 13-2. Alarmas predeterminadas de vSAN

Alarmas de vSAN	Descripción
Licencia por tiempo limitado de vSAN caducada	Permite supervisar las licencias de prueba de vSAN.
Error de registro o cancelación del registro de un proveedor VASA en un host vSAN	Permite registrar proveedores de VASA en los hosts de vSAN que generaron errores, o bien eliminarlos del registro.
Licencia de vSAN vencida	Permite supervisar las licencias de vSAN vencidas.
Errores producidos en los discos de un host vSAN	Permite supervisar errores en los dispositivos de vSAN.
Alarma de vSAN Health Service para la prueba de grupo 'Estado de clúster'	Permite supervisar el estado del clúster de vSAN.
Alarma de vSAN Health Service para la prueba de grupo 'Estado de datos'	Permite supervisar el estado de los datos del clúster de vSAN.
Alarma de vSAN Health Service para la prueba de grupo 'Estado de límites'	Permite supervisar los límites del clúster de vSAN.
Alarma de vSAN Health Service para la prueba de grupo 'Estado de red'	Permite supervisar el estado de la red de vSAN.
Alarma de vSAN Health Service para la prueba de grupo 'Estado de disco físico'	Permite supervisar el estado de los dispositivos físicos en el clúster.
Alarma de vSAN Health Service para la prueba de grupo 'Estado de HCL de vSAN'	Permite supervisar los componentes del clúster y garantizar que utilizan hardware, software y controladores admitidos.
Alarma de vSAN Health Service para la prueba de grupo 'Estado de software'	Permite supervisar el estado del software que se usa actualmente en el clúster.
Alarma de vSAN Health Service para la prueba de grupo 'Estado de vSAN inesperado'	Permite supervisar cualquier problema de estado del clúster inesperado.
Alarma de vSAN Health Service para la prueba de grupo 'Ejecución de CLOMD de vSAN'	Permite supervisar si CLOMD (Cluster Level Object Manager Daemon, Demonio de administración de objetos de nivel de clúster), que se ejecuta en hosts ESXi y es responsable de las evacuaciones y transferencias de datos, está activo o no.
Alarma de vSAN Health Service para la prueba de grupo 'Partición de clúster de vSAN'	Permite supervisar la partición del clúster de vSAN.

Para obtener información sobre supervisión de alarmas, eventos y edición de los ajustes de configuración de las alarmas actuales, consulte el documento *Supervisión y rendimiento de vSphere*.

Ver las alarmas predeterminadas de vSAN

Use las alarmas predeterminadas de vSAN para supervisar el clúster, los hosts, analizar nuevos eventos y evaluar el estado general del clúster.

Procedimiento

1 Desplácese hasta el clúster de vSAN en vSphere Web Client.

2 Haga clic en **Configure** (Configurar) y, después, haga clic en **Alarm Definitions** (Definiciones de alarma).

3 En el cuadro de búsqueda, escriba **vSAN** como término de búsqueda para mostrar las alarmas que son específicas de vSAN.

   Escriba Alarma de vSAN Health Service para buscar alarmas de vSAN Health Service.

   Se muestran las alarmas predeterminadas de vSAN.

4 En la lista de alarmas, haga clic en cada alarma para ver la definición de la alarma.

Usar las observaciones de VMkernel para la creación de alarmas

Las observaciones de VMkernel (VMkernel Observations, VOB) son eventos del sistema que pueden utilizarse para configurar alarmas de vSAN para la supervisión y la solución de los problemas de rendimiento y de la red en el clúster de vSAN. En vSAN, estos eventos se conocen como observaciones.

Identificadores de observaciones de VMware ESXi para vSAN

Cada evento de VOB está asociado con un identificador (ID). Antes de crear una alarma de vSAN en vCenter Server, deberá reconocer un identificador de VOB apropiado para el evento de vSAN para el que desee crear una alerta. Puede crear alertas en el archivo de registro de observaciones de VMware ESXi (`vobd.log`). Por ejemplo, debe usar los siguientes identificadores de VOB para crear alertas para cualquier tipo de errores de dispositivos en el clúster.

- `esx.problem.vob.vsan.lsom.diskerror`
- `esx.problem.vob.vsan.pdl.offline`

Si desea consultar la lista de identificadores de VOB para vSAN, abra el archivo `vobd.log` en el host ESXi del directorio `/var/log`. El archivo de registro contiene los siguientes identificadores de VOB que puede utilizar para crear alarmas de vSAN.

Tabla 13-3. Identificadores de VOB para vSAN

Identificador de VOB	Descripción
esx.audit.vsan.clustering.enabled	El servicio de agrupación en clústeres de vSAN está habilitado.
esx.clear.vob.vsan.pdl.online	El dispositivo de vSAN se conectó.
esx.clear.vsan.clustering.enabled	Los servicios de agrupación en clústeres de vSAN están habilitados.
esx.clear.vsan.vsan.network.available	vSAN tiene una configuración de red activa.
esx.clear.vsan.vsan.vmknic.ready	Una vmknic informada anteriormente ha obtenido una dirección IP válida.
esx.problem.vob.vsan.lsom.componentthreshold	vSAN se aproxima al límite de recuento de componentes del nodo.
esx.problem.vob.vsan.lsom.diskerror	Un dispositivo de vSAN presenta un estado de error permanente.
esx.problem.vob.vsan.lsom.diskgrouplimit	vSAN no crea un nuevo grupo de discos.
esx.problem.vob.vsan.lsom.disklimit	vSAN no agrega dispositivos nuevos a un grupo de discos.

Tabla 13-3. Identificadores de VOB para vSAN (Continua)

Identificador de VOB	Descripción
esx.problem.vob.vsan.lsom.diskunhealthy	El disco de vSAN está en mal estado.
esx.problem.vob.vsan.pdl.offline	Un dispositivo de vSAN está sin conexión.
esx.problem.vsan.clustering.disabled	Los servicios de agrupación en clústeres de vSAN están deshabilitados.
esx.problem.vsan.lsom.congestionthreshold	Se ha actualizado la congestión de SSD o la memoria de un dispositivo de vSAN.
esx.problem.vsan.net.not.ready	Se agrega una vmknic a la configuración de red de vSAN sin una dirección IP válida. Esto sucede cuando la red de vSAN no está lista.
esx.problem.vsan.net.redundancy.lost	La configuración de red de vSAN no cuenta con la redundancia necesaria.
esx.problem.vsan.no.network.connectivity	vSAN no tiene la configuración de red actual que está en uso.
esx.problem.vsan.vmknic.not.ready	Se agrega una vmknic a la configuración de red de vSAN sin una dirección IP válida.

Crear una alarma de vCenter Server para un evento de vSAN

Puede crear alarmas para supervisar eventos en el objeto seleccionado de vSAN, incluidos el clúster, los hosts, los almacenes de datos, las redes y las máquinas virtuales.

Prerequisitos

Debe tener el nivel de privilegio requerido de `Alarms.Create Alarm` o `Alarm.Modify Alarm`.

Procedimiento

1 Seleccione el objeto de vCenter Server en el inventario que desea supervisar.

2 Haga clic en la pestaña **Configure** (Configurar) > **Alarm Definitions** (Definiciones de alarma) > y haga clic en el icono ✚.

3 Introduzca un nombre y una descripción para la nueva alarma.

4 En el menú desplegable **Monitor** (Supervisar), seleccione el objeto en el que desea configurar una alarma.

5 Haga clic en el **evento específico producido en este objeto (por ejemplo, encendido de máquina virtual)** y, a continuación, haga clic en **Next** (Siguiente).

6 Haga clic en **Activadores** para agregar un evento de vSAN que activará la alarma. Las opciones de la página Triggers (Activadores) cambian según el tipo de actividad que va a supervisar.

7 Haga clic en el icono **Add** (Agregar) (✚).

8 Haga clic en la columna **Event** (Evento) y seleccione una opción desde el menú desplegable.

9 Haga clic en la columna **Status** (Estado) y seleccione una opción desde el menú desplegable.

10 (Opcional) Configure las condiciones adicionales que se deben cumplir para que se active la alarma.

a Haga clic en el icono **Add** (Agregar) para agregar un argumento.

b Haga clic en la columna **Argument** (Argumento) y seleccione una opción desde el menú desplegable.

c Haga clic en la columna **Operator** (Operador) y seleccione una opción desde el menú desplegable.

d Haga clic en el campo **Value** (Valor) e introduzca un valor en el campo de texto.

Puede agregar más de un argumento.

11 Haga clic en **Next** (Siguiente).

Ha seleccionado y configurado los activadores de alarmas.

Controlar errores y solucionar problemas en vSAN 14

Si se encuentran problemas al usar vSAN, puede usar los temas de solución de problemas. Los temas ayudan a comprender el problema y ofrecen una solución alternativa, siempre que haya una disponible.

Este capítulo cubre los siguientes temas:

Usar comandos Esxcli con vSAN

Use comandos Esxcli para obtener información sobre vSAN y para solucionar problemas del entorno de vSAN.

Están disponibles los siguientes comandos:

Comando	Descripción
`esxcli vsan network list`	Comprueba qué adaptadores de VMkernel se utilizan para la comunicación de vSAN.
`esxcli vsan storage list`	Enumera los discos de almacenamiento reclamados por vSAN.
`esxcli vsan cluster get`	Obtiene información del clúster de vSAN.
`esxcli vsan health`	Obtiene el estado de mantenimiento del clúster de vSAN.
`esxcli vsan debug`	Obtiene información de depuración del clúster de vSAN.

Los comandos `esxcli vsan debug` pueden ayudar a depurar y solucionar problemas en el clúster de vSAN, en especial, cuando vCenter Server no está disponible.

Use: `esxcli vsan debug {cmd} [cmd options]`

Comandos de depuración:

Comando	Descripción
`esxcli vsan debug disk`	Depurar discos físicos de vSAN.
`esxcli vsan debug object`	Depurar objetos de vSAN.
`esxcli vsan debug resync`	Depurar objetos de resincronización de vSAN.

Comando	Descripción
`esxcli vsan debug controller`	Depurar controladores de disco de vSAN.
`esxcli vsan debug limit`	Depurar límites de vSAN.
`esxcli vsan debug vmdk`	Depurar VMDK de vSAN.

Ejemplos de comandos `esxcli vsan debug`:

```
esxcli vsan debug disk summary get
   Overall Health: green
   Component Metadata Health: green
   Memory Pools (heaps): green
   Memory Pools (slabs): green
```

```
esxcli vsan debug disk list
UUID: 52e1d1fa-af0e-0c6c-f219-e5e1d224b469
   Name: mpx.vmhba1:C0:T1:L0
   SSD: False
   Overall Health: green
   Congestion Health:
         State: green
         Congestion Value: 0
         Congestion Area: none
   In Cmmds: true
   In Vsi: true
   Metadata Health: green
   Operational Health: green
   Space Health:
         State: green
         Capacity: 107365793792 bytes
         Used: 1434451968 bytes
         Reserved: 150994944 bytes
```

```
esxcli vsan debug object health summary get
    Health Status                                     Number Of Objects
    ------------------------------------------------  -----------------
    reduced-availability-with-no-rebuild-delay-timer                  0
    reduced-availability-with-active-rebuild                          0
    inaccessible                                                      0
    data-move                                                         0
    healthy                                                           1
    nonavailability-related-incompliance                              0
    nonavailability-related-reconfig                                  0
    reduced-availability-with-no-rebuild                              0
```

```
esxcli vsan debug object list
    Object UUID: 47cbdc58-e01c-9e33-dada-020010d5dfa3
       Version: 5
       Health: healthy
       Owner:
       Policy:
          stripeWidth: 1
          CSN: 1
          spbmProfileName: vSAN Default Storage Policy
          spbmProfileId: aa6d5a82-1c88-45da-85d3-3d74b91a5bad
          forceProvisioning: 0
          cacheReservation: 0
```

```
      proportionalCapacity: [0, 100]
      spbmProfileGenerationNumber: 0
      hostFailuresToTolerate: 1

   Configuration:
      RAID_1
         Component: 47cbdc58-6928-333f-0c51-020010d5dfa3
           Component State: ACTIVE,  Address Space(B): 273804165120 (255.00GB),
           Disk UUID: 52e95956-42cf-4d30-9cbe-763c616614d5, Disk Name: mpx.vmhba1..
           Votes: 1,  Capacity Used(B): 373293056 (0.35GB),
           Physical Capacity Used(B): 369098752 (0.34GB),  Host Name: sc-rdops...
         Component: 47cbdc58-eebf-363f-cf2b-020010d5dfa3
           Component State: ACTIVE,  Address Space(B): 273804165120 (255.00GB),
           Disk UUID: 52d11301-1720-9901-eb0a-157d68b3e4fc,  Disk Name: mpx.vmh...
           Votes: 1,  Capacity Used(B): 373293056 (0.35GB),
           Physical Capacity Used(B): 369098752 (0.34GB),  Host Name: sc-rdops-vm..
      Witness: 47cbdc58-21d2-383f-e45a-020010d5dfa3
        Component State: ACTIVE,  Address Space(B): 0 (0.00GB),
        Disk UUID: 52bfd405-160b-96ba-cf42-09da8c2d7023,  Disk Name: mpx.vmh...
        Votes: 1,  Capacity Used(B): 12582912 (0.01GB),
        Physical Capacity Used(B): 4194304 (0.00GB),  Host Name: sc-rdops-vm...

   Type: vmnamespace
   Path: /vmfs/volumes/vsan:52134fafd48ad6d6-bf03cb6af0f21b8d/New Virtual Machine
   Group UUID: 00000000-0000-0000-0000-000000000000
   Directory Name: New Virtual Machine
```

```
esxcli vsan debug controller list
    Device Name: vmhba1
       Device Display Name: LSI Logic/Symbios Logic 53c1030 PCI-X Fusion-MPT Dual Ult..
       Used By VSAN: true
       PCI ID: 1000/0030/15ad/1976
       Driver Name: mptspi
       Driver Version: 4.23.01.00-10vmw
       Max Supported Queue Depth: 127
```

```
esxcli vsan debug limit get
       Component Limit Health: green
       Max Components: 750
       Free Components: 748
       Disk Free Space Health: green
       Lowest Free Disk Space: 99 %
       Used Disk Space: 1807745024 bytes
       Used Disk Space (GB): 1.68 GB
       Total Disk Space: 107365793792 bytes
       Total Disk Space (GB): 99.99 GB
       Read Cache Free Reservation Health: green
```

```
      Reserved Read Cache Size: 0 bytes
      Reserved Read Cache Size (GB): 0.00 GB
      Total Read Cache Size: 0 bytes
      Total Read Cache Size (GB): 0.00 GB
```

```
esxcli vsan debug vmdk list
    Object: 50cbdc58-506f-c4c2-0bde-020010d5dfa3
       Health: healthy
       Type: vdisk
       Path: /vmfs/volumes/vsan:52134fafd48ad6d6-bf03cb6af0f21b8d/47cbdc58-e01c-9e33-
             dada-020010d5dfa3/New Virtual Machine.vmdk
       Directory Name: N/A
```

```
esxcli vsan debug resync list
   Object            Component              Bytes Left To Resync  GB Left To Resync
   ----------------  ---------------------  --------------------  -----------------
   31cfdc58-e68d...  Component:23d1dc58...             536870912  0.50
   31cfdc58-e68d...  Component:23d1dc58...            1073741824  1.00
   31cfdc58-e68d...  Component:23d1dc58...            1073741824  1.00
```

La configuración de vSAN en un host ESXi podría generar errores

En ciertos casos, la tarea de configurar vSAN en un host particular podría presentar error.

Problema

Un host ESXi que se une a un clúster de vSAN no tiene vSAN configurado.

Origen

Si un host no cumple con los requisitos de hardware o experimenta otros problemas, vSAN podría presentar error cuando se configura el host. Por ejemplo, una memoria insuficiente en el host podría evitar que se configure vSAN.

Solución

1. Coloque el host que provoca el error en modo de mantenimiento.
2. Mueva el host fuera del clúster de vSAN.
3. Resuelva el problema que evita que el host tenga vSAN configurado.
4. Salga del modo de mantenimiento.
5. Mueva el host de vuelta al clúster de vSAN.

Los objetos de la máquina virtual no compatibles no se vuelven compatibles instantáneamente

Cuando se usa el botón **Comprobar cumplimiento**, un objeto de máquina virtual no cambia su estado de No cumple con las normas a Cumple con las normas aunque haya recursos de vSAN disponibles y satisfaga el perfil de la máquina virtual.

Problema

Cuando usa el aprovisionamiento a la fuerza, puede aprovisionar un objeto de máquina virtual incluso cuando la directiva especificada en el perfil de máquina virtual no pueda cumplirse con los recursos disponibles en el clúster de vSAN. Se crea el objeto, pero permanece en el estado de que no cumple con la normas.

Se espera que vSAN lleve el objeto a cumplimiento de normas cuando los recursos de almacenamiento en el clúster queden disponibles, por ejemplo, cuando agrega un host. Sin embargo, el estado del objeto no cambia a que cumple con las normas inmediatamente después de que agrega recursos.

Origen

Esto se produce debido a que vSAN regula el ritmo de la reconfiguración para evitar sobrecargar el sistema. La cantidad de tiempo que se requiere para lograr el cumplimiento de normas depende de la cantidad de objetos en el clúster, la carga de E/S en el clúster y el tamaño del objeto en cuestión. En la mayoría de los casos, el cumplimiento de normas se logra en un tiempo razonable.

Problemas de configuración del clúster de vSAN

Después de cambiar la configuración de vSAN, vCenter Server realiza comprobaciones de validación para la configuración de vSAN. Las comprobaciones de validación también se realizan como parte de un proceso de sincronización de hosts. Si vCenter Server detecta problemas de configuración, muestra mensajes de error.

Problema

Los mensajes de error indican que vCenter Server ha detectado un problema con la configuración de vSAN.

Solución

Utilice los siguientes métodos para solucionar problemas de configuración de vSAN.

Tabla 14-1. Errores y soluciones en la configuración de vSAN

Error de configuración de vSAN	Solución
Un host con el servicio de VSAN habilitado no está en el clúster de vCenter	Agregue el host al clúster de vSAN. 1 Haga clic con el botón derecho y seleccione **Move To** (Mover a). 2 Seleccione el clúster de vSAN y haga clic en **Aceptar**.
Un host se encuentra en un clúster habilitado para VSAN, pero no tiene el servicio de VSAN habilitado	Compruebe si la red de vSAN está configurada y habilitada adecuadamente en el host. Consulte "Configurar la red de vSAN," página 44.
La red de VSAN no está configurada	Configure la red de vSAN. Consulte "Configurar la red de vSAN," página 44.
Un host no puede comunicarse con todos los otros nodos en el clúster habilitado para VSAN	Podría deberse a aislamiento de la red. Consulte el documento "Requisitos de red para vSAN," página 19.
Se encuentra otro host que participa en el servicio de VSAN que no es miembro del clúster de vCenter de este host.	Asegúrese de que la configuración de clúster de vSAN sea correcta y que todos los hosts de vSAN estén en la misma subred. Consulte "Diseñar la red de vSAN," página 31.

Controlar errores en vSAN

vSAN controla los errores de los dispositivos de almacenamiento, los hosts y la red en el clúster de acuerdo con la gravedad del error. Es posible diagnosticar problemas en vSAN observando el rendimiento de la red y del almacén de datos de vSAN.

Control de errores en vSAN

vSAN implementa mecanismos para indicar la presencia de errores y recompilar los datos no disponibles para la protección de datos.

Estados de error de los componentes de vSAN

En vSAN, los componentes que han generado errores pueden aparecer en estado ausente o degradado. Según el estado del componente, vSAN emplea diferentes enfoques para la recuperación de los datos de máquinas virtuales.

Asimismo, vSAN proporciona alertas en relación con el tipo de error del componente. Consulte "Usar las observaciones de VMkernel para la creación de alarmas," página 161 y "Usar las alarmas predeterminada de vSAN," página 160.

vSAN admite dos tipos de estados de error para los componentes:

Tabla 14-2. Estados de error de los componentes en vSAN

Estados de error de componente	Descripción	Recuperación	Motivo
Degraded (Degradado)	Un componente entra en estado degradado si vSAN detecta un error permanente de un componente y supone que dicho componente no va a recuperar su estado de funcionamiento.	vSAN comienza la recompilación de los componentes afectados de inmediato.	■ Error de un dispositivo flash de almacenamiento en caché ■ Error de un dispositivo magnético o de capacidad flash ■ Error de controladora de almacenamiento
Absent (Ausente)	Un componente entra en estado ausente si vSAN detecta un error temporal de un componente en un escenario en el que es posible que dicho componente recupere y restaure su estado de funcionamiento.	vSAN comienza la recompilación de los componentes ausentes si estos no están disponibles después de un tiempo de espera determinado. Como opción predeterminada, vSAN comienza la recompilación de los componentes ausentes después de 60 minutos.	■ Pérdida de conectividad de red ■ Error de un adaptador de red físico ■ Error de host ESXi ■ Dispositivo flash de almacenamiento en caché desconectado ■ Dispositivo magnético o dispositivo de capacidad flash desconectados

Examinar el estado de error de un componente

Use vSphere Web Client para examinar si un componente se encuentra en estado ausente o degradado.

Si se produce un error en el clúster, vSAN marca los componentes de un objeto como ausentes o degradados según la gravedad del error.

Procedimiento

1 En vSphere Web Client, desplácese hasta el clúster de vSAN.

2 En la pestaña **Monitor** (Supervisar), haga clic en **vSAN** y seleccione **Virtual Disks** (Discos virtuales).

   Aparecerán los directorios principales y los discos virtuales de las máquinas virtuales del clúster.

3 Seleccione un objeto de una máquina virtual.

4 En la pestaña **Physical Disk Placement** (Ubicación de discos físicos), examine la propiedad Component State (Estado de componente) de los componentes para el objeto seleccionado.

   Si se ha producido un error en el clúster de vSAN, la propiedad Estado de componente tiene el estado Ausente o Degradado.

Estados de objetos que indican problemas en vSAN

Analice el estado de cumplimiento y el estado operativo de un objeto de una máquina virtual a fin de determinar la manera en que un error en el clúster afecta a la máquina virtual.

Tabla 14-3. Estado de objeto

Tipo de estado de objeto	Descripción
Estado de cumplimiento	El estado de cumplimiento de un objeto de una máquina virtual indica si cumple con los requisitos de la directiva de almacenamiento de máquina virtual asignada.
Estado operativo	El estado operativo de un objeto puede ser correcto o incorrecto. Indica el tipo y la cantidad de errores en el clúster. El estado de un objeto es correcto si están disponibles una réplica intacta y más del 50 % de los votos del objeto. El estado de un objeto es incorrecto si no están disponibles una réplica completa o menos del 50 % de los votos del objeto. Por ejemplo, un objeto puede entrar en estado incorrecto si se produce un error de red en el clúster y un host queda aislado.

Para determinar la incidencia general de un error en una máquina virtual, analice el estado de cumplimiento y el estado operativo. Si el estado operativo sigue siendo correcto a pesar del incumplimiento del objeto, la máquina virtual puede seguir usando el almacén de datos de vSAN. Si el estado operativo es incorrecto, la máquina virtual no puede usar el almacén de datos.

Examinar el estado de un objeto en vSAN

Use vSphere Web Client para analizar si el estado de una máquina virtual es óptimo. Una máquina virtual se considera en estado óptimo cuando están disponibles una réplica del objeto de la máquina virtual y más del 50 % de los votos para un objeto.

Procedimiento

1 En vSphere Web Client, desplácese hasta el clúster de vSAN.

2 En la pestaña **Monitor** (Supervisar), haga clic en **vSAN** y seleccione **Virtual Disks** (Discos virtuales).

   Aparecerán los directorios principales y los discos virtuales de las máquinas virtuales del clúster.

3 Para un objeto de una máquina virtual, analice el valor de la propiedad Operational State (Estado operativo).

   Si el valor de Operational State (Estado operativo) es Unhealthy (Estado incorrecto), vSphere Web Client indica entre paréntesis el motivo del estado incorrecto.

Examinar el estado de cumplimiento de un objeto de una máquina virtual en vSAN

Use vSphere Web Client para analizar si un objeto de una máquina virtual cumple con la directiva de almacenamiento de máquina virtual asignada.

Procedimiento

1 Analice el estado de cumplimiento de un objeto de una máquina virtual.

   a Desplácese hasta la máquina virtual en el navegador de vSphere Web Client.

   b Desde la pestaña **Summary** (Resumen), analice el valor de la propiedad VM Storage Policy Compliance (Cumplimiento de directiva de almacenamiento de máquina virtual) en la sección VM Storage Policies (Directivas de almacenamiento de máquina virtual).

2 Analice el estado de cumplimiento de los objetos de la máquina virtual.

   a En vSphere Web Client, desplácese hasta el clúster de vSAN.

   b En la pestaña **Monitor** (Supervisar), haga clic en **vSAN** y seleccione **Virtual Disks** (Discos virtuales).

   c Seleccione un objeto de una máquina virtual.

   d Analice el valor de la propiedad Compliance Status (Estado de cumplimiento) del objeto. Si el valor de Compliance Status (Estado de cumplimiento) no es Compliant (Cumplimiento), determine la causa del incumplimiento.

   - Analice el estado operativo del objeto para comprobar si el objeto tiene un estado correcto.
   - Desde la pestaña **Compliance Failure** (Error de cumplimiento), analice los requisitos de la directiva de almacenamiento de máquina virtual que no puede cumplir el objeto.
   - En la pestaña **Physical Disk Placement** (Ubicación de discos físicos), analice el estado de los componentes del objeto.

Accesibilidad de las máquinas virtuales ante un error de vSAN

Si una máquina virtual usa almacenamiento de vSAN, su accesibilidad al almacenamiento puede cambiar según el tipo de error que se produzca en el clúster de vSAN.

Se producen cambios en la accesibilidad cuando el clúster experimenta más errores que los que tolera la directiva para una máquina virtual.

Como consecuencia de un error en el clúster de vSAN, es posible que un objeto de una máquina virtual deje de estar accesible. Un objeto no está accesible si una réplica completa del objeto afecta a todas las réplicas, ni tampoco cuando menos del 50 % de los votos del objeto están disponibles.

Según el tipo de objeto que no está accesible, las máquinas virtuales se comportan de las siguientes maneras:

Tabla 14-4. Inaccesibilidad de objetos de máquinas virtuales

Tipo de objeto	Estado de la máquina virtual	Síntomas de la máquina virtual
Espacio de nombres del directorio principal de la máquina virtual	■ Inaccesible ■ Huérfano si vCenter Server o el host ESXi no pueden acceder al archivo `.vmx` de la máquina virtual.	Es posible que el proceso de la máquina virtual se bloquee y que la máquina virtual se apague.
VMDK	Inaccesible	La máquina virtual permanece encendida, pero no se ejecutan las operaciones de E/S en el VMDK. Después de que transcurre un tiempo de espera determinado, el sistema operativo invitado termina las operaciones.

La inaccesibilidad de la máquina virtual no es un estado permanente. Una vez que se resuelve el problema subyacente y que se restauran una réplica completa y más del 50 % de los votos del objeto, automáticamente, la máquina virtual vuelve a estar disponible.

Error del dispositivo de almacenamiento en un clúster de vSAN

vSAN supervisa el rendimiento de cada dispositivo de almacenamiento y aísla de forma proactiva los dispositivos en estado incorrecto. Detecta el mal funcionamiento gradual de un dispositivo de almacenamiento y lo aísla antes de que se forme congestión en el host afectado y en todo el clúster de vSAN.

Si un disco experimenta niveles altos de latencia o congestión de forma sostenida, vSAN considera que el dispositivo es un disco en mal estado y evacúa los datos del disco. vSAN controla el disco en mal estado evacuando o recompilando los datos. No se requiere ninguna acción por parte del usuario a menos que el clúster carezca de recursos o incluya objetos inaccesibles.

Accesibilidad y estado de error de componentes

Los componentes de vSAN que residen en el dispositivo de capacidad flash o el disco magnético se marcan como ausentes.

Comportamiento de vSAN

vSAN responde de las siguientes maneras al error en el dispositivo de almacenamiento.

Parámetro	Comportamiento
Alarmas	Cada host genera una alarma siempre que se diagnostica un dispositivo en estado incorrecto. Se emite una advertencia cada vez que se sospecha que un disco tiene un estado incorrecto.
Comprobación de estado	La comprobación **Overall disk health** (Estado general de discos) emite una advertencia para el disco en mal estado.
Estado de mantenimiento	En la página Disk Management (Administración de discos), el estado de mantenimiento del disco que está funcionando mal es **Unhealthy** (En mal estado). Cuando vSAN completa la evacuación de los datos, el estado de mantenimiento es **DyingDiskEmpty**.
Rebuilding data (Reconstrucción de datos)	vSAN analiza si los hosts y los dispositivos de capacidad pueden satisfacer los requisitos de espacio y las reglas de ubicación para los objetos en el grupo de discos o el dispositivo que ha generado un error. Si está disponible un host con capacidad, vSAN inicia el proceso de recuperación de inmediato, porque los componentes se han marcado como degradados. Si hay recursos disponibles, vSAN vuelve a proteger los datos automáticamente.

Si vSAN detecta que hay un error permanente en un disco, hace una cantidad limitada de intentos por revivir el disco. Para ello, lo desmonta y vuelve a montarlo.

Dispositivo de capacidad no accesible en un clúster de vSAN

Cuando se produce un error en un dispositivo de capacidad flash o un disco magnético, vSAN evalúa la accesibilidad de los objetos en el dispositivo y los recompila en otro host si hay espacio disponible y si **Nivel primario de errores que se toleran** se establece en 1 o más.

Accesibilidad y estado de error de componentes

Los componentes de vSAN que residen en el dispositivo de capacidad flash o el disco magnético se marcan como degradados.

Comportamiento de vSAN

vSAN responde de la siguiente manera al error en el dispositivo de capacidad.

Parámetro	Comportamiento
Nivel primario de errores que se toleran	Si **Primary level of failures to tolerate** (Nivel principal de errores que se toleran) en la directiva de almacenamiento de máquina virtual es igual o superior a 1, los objetos de máquinas virtuales aún están accesibles desde otro host ESXi en el clúster. Si hay recursos disponibles, vSAN inicia una reprotección automática. Si **Primary level of failures to tolerate** (Nivel principal de errores que se toleran) se establece en 0, no se puede acceder a un objeto de máquina virtual si uno de los componentes del objeto reside en el dispositivo de capacidad con errores. Restaure la máquina virtual desde una copia de seguridad.
operaciones de E/S en el dispositivo de capacidad	vSAN detiene la ejecución de las operaciones de E/S entre 5 y 7 segundos hasta que reevalúa si un objeto aún está disponible sin el componente que ha generado un error. Si vSAN determina que el objeto aún está disponible, se reanuda la ejecución de las operaciones de E/S.
Rebuilding data (Reconstrucción de datos)	vSAN analiza si los hosts y los dispositivos de capacidad pueden satisfacer los requisitos de espacio y las reglas de ubicación para los objetos en el grupo de discos o el dispositivo que ha generado un error. Si está disponible un host con capacidad, vSAN inicia el proceso de recuperación de inmediato, porque los componentes se han marcado como degradados. Si hay recursos disponibles, se producirá una reprotección automática.

Un dispositivo flash de almacenamiento en caché capacidad no accesible en un clúster de vSAN

Cuando se produce un error en un dispositivo flash de almacenamiento en caché, vSAN evalúa la accesibilidad de los objetos en el grupo de discos que contiene el dispositivo de memoria caché y los recompila en otro host si es posible y si **Nivel primario de errores que se toleran** se establece en 1 o más.

Accesibilidad y estado de error de componentes

Los dispositivos de memoria caché y de capacidad que residen en el grupo de discos (por ejemplo, discos magnéticos) se marcan como degradados. vSAN interpreta el error de un solo dispositivo flash de almacenamiento en caché como un error de todo el grupo de discos.

Comportamiento de vSAN

vSAN responde de la siguiente manera al error en el dispositivo flash de almacenamiento en caché:

Parámetro	Comportamiento
Nivel primario de errores que se toleran	Si **Primary level of failures to tolerate** (Nivel principal de errores que se toleran) en la directiva de almacenamiento de máquina virtual es igual o superior a 1, los objetos de máquinas virtuales aún están accesibles desde otro host ESXi en el clúster. Si hay recursos disponibles, vSAN inicia una reprotección automática. Si **Primary level of failures to tolerate** (Nivel principal de errores que se toleran) se establece en 0, no se puede acceder a un objeto de máquina virtual si uno de los componentes del objeto está en el grupo de discos con errores.
operaciones de E/S en el grupo de discos	vSAN detiene la ejecución de las operaciones de E/S entre 5 y 7 segundos hasta que reevalúa si un objeto aún está disponible sin el componente que ha generado un error. Si vSAN determina que el objeto aún está disponible, se reanuda la ejecución de las operaciones de E/S.
Rebuilding data (Reconstrucción de datos)	vSAN analiza si los hosts y los dispositivos de capacidad pueden satisfacer los requisitos de espacio y las reglas de ubicación para los objetos en el grupo de discos o el dispositivo que ha generado un error. Si está disponible un host con capacidad, vSAN inicia el proceso de recuperación de inmediato, porque los componentes se han marcado como degradados.

Un host no responde en un clúster de vSAN

Si un host deja de responder debido a un error o un reinicio del host, vSAN espera hasta que el host se recupere. Luego, vSAN vuelve a compilar los componentes en el host en otra ubicación del clúster.

Accesibilidad y estado de error de componentes

Los componentes de vSAN que residen en el host se marcan como ausentes.

Comportamiento de vSAN

vSAN responde de la siguiente manera al error del host:

Parámetro	Comportamiento
Nivel primario de errores que se toleran	Si **Primary level of failures to tolerate** (Nivel principal de errores que se toleran) en la directiva de almacenamiento de máquina virtual es igual o superior a 1, los objetos de máquinas virtuales aún están accesibles desde otro host ESXi en el clúster. Si hay recursos disponibles, vSAN inicia una reprotección automática. Si **Primary level of failures to tolerate** (Nivel principal de errores que se toleran) se establece en 0, no puede accederse a un objeto de máquina virtual si los componentes del objeto residen en el host en el que se produjo el error.
I/O operations on the host (Operaciones de E/S en el host)	vSAN detiene la ejecución de las operaciones de E/S entre 5 y 7 segundos hasta que reevalúa si un objeto aún está disponible sin el componente que ha generado un error. Si vSAN determina que el objeto aún está disponible, se reanuda la ejecución de las operaciones de E/S.
Rebuilding data (Reconstrucción de datos)	Si el host no vuelve a unirse al clúster en el transcurso de 60 minutos, vSAN analiza si algunos de los otros hosts del clúster pueden satisfacer los requisitos de memoria caché, espacio y reglas de ubicación para los objetos del host que está inaccesible. Si está disponible un host con esas características, vSAN inicia el proceso de recuperación. Si el host vuelve a unirse al clúster después de 60 minutos y la recuperación ha comenzado, vSAN evalúa si debe continuar con la recuperación o interrumpirla y volver a sincronizar los componentes originales.

Se ha perdido la conectividad de red en el clúster de vSAN

Cuando se pierde la conectividad de red entre los hosts del clúster, vSAN determina cuál es la partición activa y vuelve a compilar los componentes a partir de la partición aislada en la partición activa si no se restaura la conectividad.

Accesibilidad y estado de error de componentes

vSAN determina cuál es la partición en la que están disponibles más del 50 % de los votos de un objeto. Los componentes en los hosts aislados se marcan como ausentes.

Comportamiento de vSAN

vSAN responde de la siguiente manera a un error de red:

Parámetro	Comportamiento
Nivel primario de errores que se toleran	Si **Primary level of failures to tolerate** (Nivel principal de errores que se toleran) en la directiva de almacenamiento de máquina virtual es igual o superior a 1, los objetos de máquinas virtuales aún están accesibles desde otro host ESXi en el clúster. Si hay recursos disponibles, vSAN inicia una reprotección automática. Si **Primary level of failures to tolerate** (Nivel principal de errores que se toleran) se establece en 0, no puede accederse a un objeto de máquina virtual si los componentes del objeto están en los hosts aislados.
operaciones de E/S en los hosts aislados	vSAN detiene la ejecución de las operaciones de E/S entre 5 y 7 segundos hasta que reevalúa si un objeto aún está disponible sin el componente que ha generado un error. Si vSAN determina que el objeto aún está disponible, se reanuda la ejecución de las operaciones de E/S.
Rebuilding data (Reconstrucción de datos)	Si el host vuelve a unirse al clúster en el transcurso de 60 minutos, vSAN sincroniza los componentes del host. Si el host no vuelve a unirse al clúster en el transcurso de 60 minutos, vSAN analiza si algunos de los otros hosts del clúster pueden satisfacer los requisitos de memoria caché, espacio y reglas de ubicación para los objetos del host que está inaccesible. Si está disponible un host con esas características, vSAN inicia el proceso de recuperación. Si el host vuelve a unirse al clúster después de 60 minutos y la recuperación ha comenzado, vSAN evalúa si debe continuar con la recuperación o interrumpirla y volver a sincronizar los componentes originales.

Error de una controladora de almacenamiento en un clúster de vSAN

Cuando se produce un error en una controladora de almacenamiento, vSAN evalúa la accesibilidad de los objetos en los grupos de discos asociados a la controladora y los recompila en otro host.

Síntomas

Si un host contiene una sola controladora de almacenamiento y varios grupos de discos, y se produce un error en todos los dispositivos de todos los grupos de discos, se puede suponer que un error en la controladora de almacenamiento común es la causa de origen. Analice los mensajes de registro de VMkernel para determinar la naturaleza del error.

Accesibilidad y estado de error de componentes

Cuando se produce un error en una controladora de almacenamiento, los componentes de los dispositivos flash de almacenamiento en caché y los dispositivos de capacidad en todos los grupos de discos que están conectados a la controladora se marcan como degradados.

Si un host contiene varias controladoras y solo los dispositivos que están asociados a una controladora individual están inaccesibles, se puede suponer que se ha producido un error en esta controladora.

Comportamiento de vSAN

vSAN responde de la siguiente manera a un error en una controladora de almacenamiento:

Parámetro	Comportamiento
Nivel primario de errores que se toleran	Si **Primary level of failures to tolerate** (Nivel principal de errores que se toleran) en la directiva de almacenamiento de máquina virtual es igual o superior a 1, los objetos de máquinas virtuales aún están accesibles desde otro host ESXi en el clúster. Si hay recursos disponibles, vSAN inicia una reprotección automática. Si **Primary level of failures to tolerate** (Nivel principal de errores que se toleran) se establece en 0, no puede accederse a un objeto de máquina virtual si los componentes del objeto están en los grupos de discos que están conectados a la controladora de almacenamiento.
Rebuilding data (Reconstrucción de datos)	vSAN analiza si los hosts y los dispositivos de capacidad pueden satisfacer los requisitos de espacio y las reglas de ubicación para los objetos en el grupo de discos o el dispositivo que ha generado un error. Si está disponible un host con capacidad, vSAN inicia el proceso de recuperación de inmediato, porque los componentes se han marcado como degradados.

Error o conexión de red perdida en sitio de clúster ampliado

Un clúster ampliado de vSAN administra los errores que se producen debido a la pérdida de una conexión de red entre sitios o la pérdida temporal de un sitio.

Control de errores de clúster ampliado

En la mayoría de los casos, el clúster ampliado continúa funcionando durante un error y se recupera de manera automática después de que se resuelve el error.

Tabla 14-5. Cómo el clúster ampliado controla errores

Tipo de error	Comportamiento
Pérdida de conexión de red entre sitios activos	Si se produce un error en la conexión de red entre dos sitios activos, el host testigo y el sitio preferido continúan brindando operaciones de almacenamiento y mantienen la información disponible. Cuando se restablece la conexión de red, los dos sitios activos se vuelven a sincronizar.
Error o conexión de red perdida en sitio secundario	Si el sitio secundario queda sin conexión o aislado del sitio preferido y del host testigo, el host testigo y el sitio preferido continúan brindando operaciones de almacenamiento y mantienen la información disponible. Cuando el sitio secundario regresa al clúster, los dos sitios activos se vuelven a sincronizar.
Error o conexión de red perdida en sitio preferido	Si el sitio preferido queda sin conexión o aislado del sitio secundario y del host testigo, el sitio secundario continúa con las operaciones de almacenamiento siempre que se mantenga conectado al host testigo. Cuando el sitio preferido regresa al clúster, los dos sitios activos se vuelven a sincronizar.
Error o conexión de red perdida en host testigo	Si el host testigo queda sin conexión o aislado del sitio preferido o del sitio secundario, los objetos se vuelven no compatibles, pero la información sigue estando disponible. Las máquinas virtuales que se encuentran en ejecución no se verán afectadas.

Solucionar problemas de vSAN

Examine el rendimiento y la accesibilidad de las máquinas virtuales para diagnosticar problemas en el clúster de vSAN.

Cotejar los controladores, el firmware y las controladoras de E/S de almacenamiento con la *Guía de compatibilidad de VMware*

Utilice vSAN Health Service para comprobar si los componentes de hardware, los controladores y el firmware son compatibles con vSAN.

El uso de componentes de hardware, controladores y firmware incompatibles con vSAN puede ocasionar problemas en el funcionamiento del clúster de vSAN y de las máquinas virtuales que se ejecutan en él.

Las comprobaciones de estado de compatibilidad del hardware verifican el hardware en comparación con la *Guía de compatibilidad de VMware*. Para obtener más información sobre el uso de vSAN Health Service, consulte "Supervisar el estado de vSAN," página 150.

Examinar el rendimiento en un clúster de vSAN

Supervise el rendimiento de las máquinas virtuales, los hosts y el almacén de datos de vSAN a fin de identificar posibles problemas de almacenamiento.

Supervise regularmente los siguientes indicadores de rendimiento para identificar errores en el almacenamiento de vSAN, por ejemplo, mediante las tablas de rendimiento de vSphere Web Client:

- Almacén de datos. Tasa de las operaciones de E/S en el almacén de datos agregado.

- Máquina virtual. Operaciones de E/S, uso de memoria y CPU, capacidad de proceso y ancho de banda de red.

Puede utilizar el servicio de rendimiento de vSAN para acceder a tablas de rendimiento detalladas. Para obtener información sobre el uso del servicio de rendimiento, consulte "Supervisar el rendimiento de vSAN," página 153. Para obtener más información sobre el uso de los datos de rendimiento en un clúster de vSAN, consulte la *Manual de referencia de solución de problemas de vSAN*.

Estado de configuración errónea de red en un clúster de vSAN

Después de habilitar vSAN en un clúster, el almacén de datos no se ensambla correctamente debido a la detección de una configuración errónea de la red.

Problema

Después de habilitar vSAN en un clúster, en la pestaña **Resumen** del clúster, el valor del estado de red para vSAN aparece como `Configuración errónea detectada`.

Origen

Uno de los miembros del clúster o más no pueden comunicarse debido a uno de los motivos siguientes:

- Un host del clúster no tiene un adaptador de VMkernel para vSAN.
- Los hosts no pueden conectarse entre sí en la red.

Solución

Una a los miembros del clúster a la misma red. Consulte "Configurar la red de vSAN," página 44.

Una máquina virtual aparece con el estado Incumplimiento, Inaccesible o Huérfana en vSAN

El estado que se muestra para una máquina virtual que almacena datos en un almacén de datos de vSAN es Incumplimiento, Inaccesible o Huérfana debido a errores en el clúster de vSAN.

Problema

Una máquina virtual de un almacén de datos de vSAN tiene uno de los estados siguientes, lo que indica un error en el clúster de vSAN.

- La máquina virtual presenta un incumplimiento y el estado de algunos de sus objetos es Non-Compliant (Incumplimiento). Consulte "Examinar el estado de cumplimiento de un objeto de una máquina virtual en vSAN," página 172.
- El objeto de la máquina virtual está inaccesible o huérfano. Consulte "Examinar el estado de error de un componente," página 170.

Si una réplica de un objeto aún está disponible en otro host, vSAN reenvía las operaciones de E/S de la máquina virtual a la réplica.

Origen

Si el objeto de la máquina virtual ya no puede cumplir con el requisito de la directiva de almacenamiento de máquina virtual asignada, vSAN considera que este presenta un incumplimiento. Por ejemplo, es posible que un host pierda temporalmente la conectividad. Consulte "Estados de objetos que indican problemas en vSAN," página 171.

Si vSAN no puede ubicar una réplica completa o más del 50 % de los votos para el objeto, la máquina virtual deja de estar accesible. Si vSAN detecta que el archivo `.vmx` no está accesible porque el espacio de nombres del directorio principal de la máquina virtual está dañado, la máquina virtual queda huérfana. Consulte "Accesibilidad de las máquinas virtuales ante un error de vSAN," página 172.

Solución

Si el clúster contiene recursos suficientes, vSAN recupera los objetos dañados de manera automática en caso de que el error sea permanente.

Si el clúster no tiene recursos suficientes para reconstruir los objetos dañados, debe extender el espacio del clúster. Consulte "Expandir la capacidad y el rendimiento de un clúster de vSAN," página 120 y "Agregar un host al clúster de vSAN," página 120.

Error al intentar crear una máquina virtual en vSAN

Al intentar implementar una máquina virtual en un clúster de vSAN, se produce un error en la operación, según el cual no es posible crear la máquina virtual.

Problema

Se produce un error en la operación de creación de la máquina virtual y se genera el estado de error: `Cannot complete file creation operation` (No se puede completar la operación de creación de archivo).

Origen

El error en la implementación de una máquina virtual en vSAN puede atribuirse a diversos motivos.

- vSAN no puede asignar espacio para las directivas de almacenamiento de la máquina virtual y los objetos de la máquina virtual. Este error puede producirse si el almacén de datos no dispone de capacidad útil suficiente, por ejemplo, si un disco físico se desconecta temporalmente del host.
- La máquina virtual tiene discos virtuales muy grandes y los hosts del clúster no pueden proporcionar almacenamiento para dichos discos de acuerdo con las reglas de ubicación de la directiva de almacenamiento de la máquina virtual.

  Por ejemplo, si **Nivel primario de errores que se toleran** en la directiva de almacenamiento de máquina virtual se establece en 1, vSAN debe almacenar dos réplicas de un disco virtual en el clúster, cada una en un host diferente. Es posible que el almacén de datos disponga de este espacio después de combinar el espacio libre en todos los hosts del clúster. Sin embargo, no puede haber dos hosts disponibles en el clúster, cada uno de los cuales proporciona espacio suficiente para almacenar una réplica separada del disco virtual.

  vSAN no transfiere componentes entre hosts ni grupos de discos a fin de liberar espacio para una réplica nueva, pese a que el clúster puede contener espacio suficiente para aprovisionar la máquina virtual nueva.

Solución

◆ Compruebe el estado de los dispositivos de capacidad del clúster.

  a En vSphere Web Client, desplácese hasta el clúster de vSAN.

  b En la pestaña **Monitor** (Supervisar), haga clic en **vSAN** y seleccione **Physical Disks** (Discos físicos).

  c Examine la capacidad y el estado de mantenimiento de los dispositivos incluidos en los hosts del clúster.

Error de configuración de clúster ampliado al agregar un host

Antes de agregar hosts nuevos a un clúster ampliado, deben conectarse todos los hosts actuales. Si se desconecta un host actual, la configuración del nuevo host queda incompleta.

Problema

Después de agregar un host nuevo a un clúster ampliado donde algunos hosts están desconectados, el estado de configuración para vSAN aparece como `Se desconfiguró el agente de unidifusión en el host` en la pestaña Resumen del clúster.

Origen

Cuando se une un host nuevo a un clúster ampliado, vSAN debe actualizar la configuración en todos los hosts del clúster. Si uno o más hosts están desconectados de vCenter Server, se produce un error en la actualización. El host nuevo se une en forma satisfactoria al clúster, pero la configuración queda incompleta.

Solución

Compruebe que todos los hosts estén conectados a vCenter Server y haga clic en el vínculo provisto en el mensaje de estado de configuración para actualizar la configuración del host nuevo.

Si no puede volver a unir el host desconectado, quite el host desconectado del clúster y haga clic en el vínculo provisto en el mensaje de estado de configuración para actualizar la configuración del host nuevo.

Error de configuración de clúster ampliado al usar RVC para agregar un host

Si usa la herramienta RVC para agregar un host nuevo a un clúster ampliado, la configuración del host nuevo queda incompleta.

Problema

Después de usar la herramienta RVC para agregar un host nuevo a un clúster ampliado, el estado de configuración de vSAN aparece como `Se desconfiguró el agente de unidifusión en el host` en la pestaña Resumen del clúster.

Origen

Cuando se une un host nuevo a un clúster ampliado, vSAN debe actualizar la configuración en todos los hosts del clúster. Si usa la herramienta RVC para agregar el host, no se produce la actualización. El host nuevo se une en forma satisfactoria al clúster, pero la configuración queda incompleta.

Solución

Compruebe que todos los hosts estén conectados a vCenter Server y haga clic en el vínculo provisto en el mensaje de estado de configuración para actualizar la configuración del host nuevo.

No se puede agregar o quitar el host testigo en un clúster ampliado

Antes de agregar o quitar el host testigo en un clúster ampliado, deben conectarse todos los hosts actuales. Si se desconecta un host actual no se puede agregar o quitar el host testigo.

Problema

Cuando se agrega o quita un host testigo en un clúster ampliado donde algunos hosts están desconectados, se producen errores en la operación y se genera el estado de error siguiente: `The operation is not allowed in the current state. Not all hosts in the cluster are connected to Virtual Center` (La operación no está permitida en el estado actual. No todos los hosts del clúster están conectados con Virtual Center).

Origen

Cuando el host testigo se une a un clúster ampliado o lo abandona, vSAN debe actualizar la configuración en todos los hosts del clúster. Si uno o más hosts están desconectados de vCenter Server, no se puede agregar o quitar el host testigo.

Solución

Compruebe que todos los hosts estén conectados a vCenter Server, y vuelva a intentar la operación. Si no puede volver a unir el host desconectado, quite el host desconectado del clúster para poder agregar o quitar el host testigo.

El grupo de discos se bloquea

En un clúster de vSAN cifrado, cuando se pierde la comunicación entre un host y KMS, el grupo de discos se puede bloquear si se reinicia el host.

Problema

vSAN bloquea los grupos de discos de un host cuando el host se reinicia y no puede obtener la KEK del servidor KMS. Los discos se comportan como si se hubieran desmontado. Ya no se puede acceder a los objetos en los discos.

Para ver el estado de mantenimiento de un grupo de discos, consulte la página Disk Management (Administración de discos) en vSphere Web Client. Se emitirá una advertencia de comprobación de estado de cifrado para informar que existe un disco bloqueado.

Origen

Los hosts de un clúster de vSAN cifrado no almacenan la KEK en disco. Si un host se reinicia y no puede obtener la KEK del servidor KMS, vSAN bloquea los grupos de discos del host.

Solución

Para salir del estado de bloqueo, debe restaurar la comunicación con el KMS y restablecer la relación de confianza.

Reemplazar componentes de hardware existentes

En determinadas condiciones, se deben reemplazar componentes de hardware, controladores, firmware y controladoras de E/S de almacenamiento en el clúster de vSAN.

En vSAN, se deben reemplazar los dispositivos de hardware al detectar errores o si es necesario actualizar el clúster.

Reemplazar un dispositivo flash de almacenamiento en caché en un host

Debe reemplazar un dispositivo flash de almacenamiento en caché si detecta un error o cuando debe actualizarlo. Antes de desconectar un dispositivo flash del host, debe quitarlo manualmente de vSAN.

ADVERTENCIA: Si retira el dispositivo flash de almacenamiento en caché sin antes quitarlo de vSAN, vSAN usa una cantidad de memoria caché menor que la esperada. Como consecuencia, el rendimiento del clúster se degrada.

Al reemplazar un dispositivo flash de almacenamiento en caché, las máquinas virtuales del grupo de discos dejan de estar accesibles y los componentes del grupo se marcan como degradados. Consulte "Un dispositivo flash de almacenamiento en caché capacidad no accesible en un clúster de vSAN," página 174.

Prerequisitos

- Compruebe que las controladoras de almacenamiento en los hosts estén configuradas en modo de acceso directo y que admitan la característica de conexión en caliente.

  Si las controladoras de almacenamiento están configuradas en modo de RAID 0, consulte la documentación del proveedor para obtener información sobre cómo agregar y quitar dispositivos.

- Si actualiza el dispositivo flash de almacenamiento en caché, compruebe los siguientes requisitos:
  - Si actualiza el dispositivo flash de almacenamiento en caché, compruebe que el clúster contenga espacio suficiente para migrar los datos desde el grupo de discos que está asociado con el dispositivo flash.
  - Coloque el host en modo de mantenimiento. Consulte "Poner un miembro de un clúster de vSAN en modo de mantenimiento," página 124.

Procedimiento

1. En vSphere Web Client, desplácese hasta el clúster de vSAN.
2. En la pestaña **Configure** (Configurar), haga clic en **Disk Management** (Administración de discos) en vSAN.
3. Seleccione el grupo de discos que contiene el dispositivo que desea reemplazar.
4. Seleccione el dispositivo flash de almacenamiento en caché y haga clic en **Remove selected disk(s) from disk group** (Quitar discos seleccionados del grupo de discos).

Después de que el dispositivo flash de almacenamiento en caché se elimine del clúster de vSAN, los detalles del clúster reflejan los ajustes de configuración y la capacidad actuales del clúster. vSAN descarta los miembros de grupos de discos, elimina las particiones y quita los datos obsoletos de todos los dispositivos.

Qué hacer a continuación

1. Agregue un nuevo dispositivo al host.

   El host detecta el dispositivo de manera automática.
2. Si el host no puede detectar el dispositivo, vuelva a examinar el dispositivo.

Reemplazar un dispositivo de capacidad

Debe reemplazar un dispositivo de capacidad flash o un disco magnético si detecta un error o al actualizar el dispositivo. Antes de quitar físicamente el dispositivo del host, debe eliminarlo manualmente de vSAN.

Al desconectar un dispositivo de capacidad sin quitarlo del clúster de vSAN, las máquinas virtuales del grupo de discos dejan de estar accesibles y los componentes del grupo se marcan como ausentes.

Si se produce un error en el dispositivo de capacidad, las máquinas virtuales dejan de estar accesibles y los componentes del grupo se marcan como degradados. Consulte “Dispositivo de capacidad no accesible en un clúster de vSAN,” página 173.

Prerequisitos

- Compruebe que las controladoras de almacenamiento en los hosts estén configuradas en modo de acceso directo y que admitan la característica de conexión en caliente.

  Si las controladoras de almacenamiento están configuradas en modo de RAID 0, consulte la documentación del proveedor para obtener información sobre cómo agregar y quitar dispositivos.
- Si actualiza el dispositivo de capacidad, compruebe los siguientes requisitos:
  - Compruebe que el clúster contenga suficiente espacio para migrar los datos del dispositivo de capacidad.
  - Coloque el host en modo de mantenimiento. Consulte “Poner un miembro de un clúster de vSAN en modo de mantenimiento,” página 124.

Procedimiento

1. En vSphere Web Client, desplácese hasta el clúster de vSAN.
2. En la pestaña **Configure** (Configurar), haga clic en **Disk Management** (Administración de discos) en vSAN.
3. Seleccione el grupo de discos que contiene el dispositivo que desea reemplazar.
4. Seleccione el dispositivo de capacidad flash o el disco magnético y haga clic en **Remove selected disk(s) from disk group** (Quitar discos seleccionados del grupo de discos).

Qué hacer a continuación

1 Agregue un nuevo dispositivo al host.

El host detecta el dispositivo de manera automática.

2 Si el host no puede detectar el dispositivo, vuelva a examinar el dispositivo.

Quitar un dispositivo de un host mediante un comando ESXCLI

Si detecta un dispositivo de almacenamiento que genera un error o si actualiza un dispositivo, puede quitarlo manualmente de un host mediante un comando ESXCLI.

Si quita un dispositivo flash de almacenamiento en caché, vSAN elimina el grupo de discos asociado con el dispositivo flash y todos sus dispositivos miembros.

Prerequisitos

Compruebe que las controladoras de almacenamiento en los hosts estén configuradas en modo de acceso directo y que admitan la característica de conexión en caliente.

Si las controladoras de almacenamiento están configuradas en modo de RAID 0, consulte la documentación del proveedor para obtener información sobre cómo agregar y quitar dispositivos.

Procedimiento

1 Abra una conexión SSH al host ESXi.

2 Para identificar el identificador del dispositivo que presenta el error, ejecute este comando y obtenga el ID del dispositivo de la salida.

```
esxcli vsan storage list
```

3 Para quitar un dispositivo de vSAN, ejecute el siguiente comando.

```
esxcli vsan storage remove -d device_id
```

Qué hacer a continuación

1 Agregue un nuevo dispositivo al host.

El host detecta el dispositivo de manera automática.

2 Si el host no puede detectar el dispositivo, vuelva a examinar el dispositivo.

Apagar el clúster de vSAN

Cuando sea necesario, puede apagar el clúster de vSAN completo.

Si tiene planificado apagar el clúster de vSAN, no es necesario que deshabilite vSAN manualmente en el clúster.

Procedimiento

1 Apague todas las máquinas virtuales (VM) que se ejecutan en el clúster de vSAN.

2 Ponga los hosts ESXi en modo de mantenimiento.

   a Haga clic con el botón derecho en el host y seleccione **Enter Maintenance Mode** (Entrar en modo de mantenimiento).

   b Seleccione el modo de evacuación **No data migration** (Sin migración de datos) y haga clic en **OK** (Aceptar).

3 En el asistente Confirm Maintenance Mode (Confirmar modo de mantenimiento), anule la selección de la casilla **Move powered-off and suspended virtual machines to other hosts in the cluster** (Transferir todas las máquinas virtuales apagadas y suspendidas a otros hosts del clúster).

   Al anular la selección de esta casilla, vSAN no migra las máquinas virtuales a otros hosts. Si tiene planificado apagar el clúster completo y poner todos los hosts en modo de mantenimiento, no es necesario que transfiera ni que migre los objetos de almacenamiento de máquina virtual a otros hosts u otros dispositivos del clúster.

4 Una vez que los hosts hayan entrado correctamente en el modo de mantenimiento, apáguelos.

5 Encienda los hosts ESXi.

   a En el sistema físico en el que está instalado ESXi, presione el botón de energía hasta que comience la secuencia de encendido.

      El host ESXi se inicia, busca las máquinas virtuales correspondientes y funciona con normalidad.

   Después de encender los hosts, el clúster de vSAN se recrea de manera automática.

   Si se desplaza hasta el host ESXi y hace clic en **Summary** (Resumen), posiblemente vea que el valor de estado de red para el clúster aparece como `Misconfiguration detected` (Configuración errónea detectada).

   Puede ignorar el mensaje de estado si no realizó cambios en la configuración de la red y el clúster de vSAN funcionaba con normalidad antes de apagar el clúster. El mensaje desaparece después de unir, al menos, tres hosts al clúster.

6 Saque los hosts del modo de mantenimiento.

7 Reinicie las máquinas virtuales.

Índice

S

T

U

V